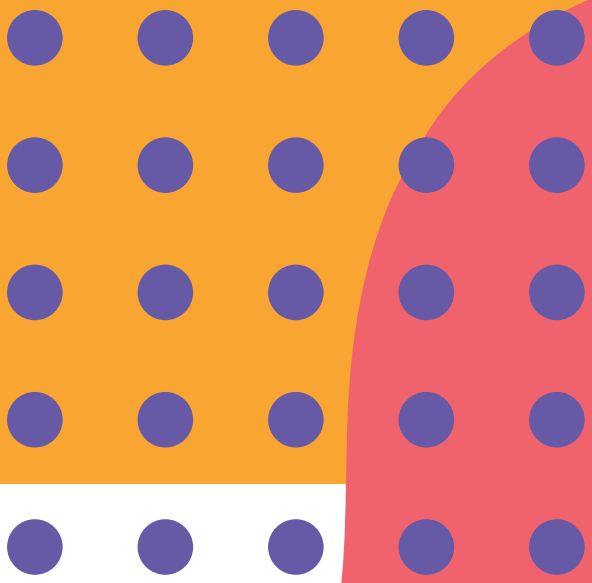
DESINFORMAÇÃO



ENFRENTAMENTO À DESINFORMAÇÃO

DEMOCRACIA SEFAZSEM DESINFORMAÇÃO

TRE-SP

CARTILHA DA DESINFORMAÇÃO

SUMÁRIO

DISSEMINAÇÃO

Após as Eleições 2018, o combate à desinformação ganhou relevância e passou a envolver um grande número de pessoas e instituições. Mas a preocupação com o tema não é nova na Justiça Eleitoral. A distribuição deliberada de boatos, visando a beneficiar ou prejudicar candidatos, é algo antigo e combatido pela legislação. A novidade é a grande capacidade de propagação dessas notícias com o advento da internet.

Uma das principais maneiras de disseminação é por meio dos chamados “bots”, ou “robôs”, na tradução do inglês. Trata-se de ferramentas automatizadas para disseminar informação, que podem ser empregadas com dois objetivos: criar conteúdo nas redes sociais ou aumentar de forma artificial a repercussão de certas informações, com curtidas e outras interações, dando a falsa impressão de que o assunto é válido e relevante.

Se o comportamento das pessoas não é favorável à checagem das informações recebidas, os robôs têm ainda mais sucesso, e os boatos podem ir passando de celular a celular até se tornarem uma bola de neve.

O problema, vale destacar, não é exclusivo do Brasil. A análise das eleições nos Estados Unidos em 2016 e na França em 2017 mostra a força que a desinformação pode vir a ter. Para combatê-la, é essencial, em primeiro lugar, a participação do próprio eleitor. Estudos da Teoria da Comunicação apontam que a internet mudou a forma de se trocar informações: o monopólio do gatekeeper, quem define aquilo que será noticiado, saiu das mãos das grandes mídias e se estendeu a qualquer pessoa com acesso à rede.

Cada cidadão, no momento em que curte ou republica uma informação no Twitter, no Facebook ou no WhatsApp, assume a responsabilidade de atuar como aquele “guardião”, passando os dados a uma série de pessoas com que se relaciona. Estas os replicarão a outros grupos de contatos, em um efeito multiplicador.

Não pode ser a Justiça Eleitoral - que é inerte e, como regra, deve ser provocada para agir - a encarregada de acabar com esse efeito. Ela deve atuar de forma repressiva, buscando minimizar as consequências da desinformação em cada caso concreto, e não de forma preventiva, o que, no limite, poderia configurar censura à garantia constitucional da liberdade de expressão.

Por isso, a participação do eleitor é fundamental. Ele não deve curtir, postar ou republicar informações que podem ser falsas. Para fazer a verificação,

recomenda-se ficar atento a alguns indícios: considerar a fonte e o autor da notícia, pesquisando se são confiáveis e se a informação está publicada também em sites com boa reputação; conferir a atualidade da data, pois muitas vezes são reaproveitadas matérias antigas por má-fé; ler a notícia inteira, porque ela pode não ter relação com o título chamativo; consultar as fontes de apoio, clicando nos demais links do material para ver se também são noticiosos. Na hora de fazer a checagem, os órgãos de imprensa e as agências de fact-checking, que têm realizado um relevante trabalho na checagem de fatos, especialmente no período eleitoral, são importantes aliados.

Por fim, os candidatos e os partidos políticos também têm grande responsabilidade no tema. Não devem patrocinar ou estimular notícias falsas, sob pena de incorrerem em crimes estabelecidos no Código Eleitoral.

Com o esforço de todos os agentes citados, pode ser construída uma eleição íntegra, sem interferências externas, na qual prevaleçam o voto esclarecido dos eleitores e a paridade de armas entre os candidatos.

QUESTÕES-ALVO DA DESINFORMAÇÃO

Embora deva manter uma posição inerte no que toca aos processos cujo assunto é desinformação, a Justiça Eleitoral vem realizando ações para combater a sua influência no resultado dos pleitos. Em 2018, por exemplo, o Tribunal Regional Eleitoral de São Paulo (TRE-SP) organizou reuniões com postulantes ao cargo de governador do Estado para fazer um pacto antipropagação de desinformação na campanha e realizou audiência pública para comprovação da integridade de urna eletrônica que foi contestada no dia do voto.

A segurança da urna é, aliás, um dos principais temas alvos de boatos. O dispositivo é totalmente seguro e utilizado há mais de 20 anos em eleições em todo o país. A urna eletrônica foi desenvolvida por um projeto de engenharia de propriedade do Tribunal Superior Eleitoral (TSE). As empresas que vencem o processo licitatório para construí-la simplesmente materializam esse projeto. Além disso, a urna não é vulnerável a ataques externos, pois foi concebida para ser um equipamento sem nenhuma ligação ou conectividade com dispositivo de rede, seja ele convencional ou sem fio.

Mesmo fora do período eleitoral, a urna é submetida a testes públicos de segurança do voto informatizado, realizados regularmente pelo TSE, conforme a Resolução nº 23.444/2015. Segundo afirma o secretário de Tecnologia da Informação do Tribunal, Giuseppe Janino, “os testes de segurança são um evento inédito no mundo. Nenhum país faz o que a Justiça Eleitoral brasileira faz: abrir seu sistema eleitoral, seja ele informatizado ou não, para que potenciais hackers tentem derrubar as barreiras de segurança”.

Durante a eleição, nesse contexto, não é possível executar qualquer tipo de software adulterado na urna eletrônica. Em um computador comum, o primeiro componente a entrar em operação é a BIOS (Sistema Básico de Entrada e Saída), mecanismo que faz verificações gerais de dispositivos no ambiente computacional. Na urna, antes mesmo de inicializar a BIOS, é instalado um dispositivo físico chamado hardware de segurança, que é protegido fisicamente e se autodestrói com qualquer tentativa de fraude. Nesse dispositivo, estão inseridas chaves públicas dos softwares e arquivos gerados na cerimônia de lacração.

Essa Cerimônia Pública de geração de mídias, preparação e lacração das urnas eletrônicas é realizada pelos TREs às vésperas das eleições. Nesse evento, todas as mídias da urna são geradas, e o software acompanhado dos dados de eleitores

e candidatos é carregado no equipamento, que, por fim, recebe lacres físicos numerados. Em seguida, a urna é programada para habilitar a votação apenas no dia da eleição e durante o período de votação. Ao final da cerimônia, é feita a lacração física do compartimento de cada uma, com selo fabricado pela Casa da Moeda. Todos esses procedimentos estão sujeitos à fiscalização do Ministério Público (MP), da Ordem dos Advogados do Brasil (OAB), dos partidos políticos e das coligações, pois se trata de um evento público.

No dia da eleição, após encerrada a votação, a urna imediatamente faz a apuração dos votos da seção e, em seguida, imprime várias vias do Boletim de Urna (BU), com o resultado de cada seção. A partir desse momento, o resultado torna-se público, podendo ser verificado por qualquer pessoa, sobretudo pelos fiscais de partido e eleitores.

Em resumo, há inúmeras ferramentas que garantem a integridade, a irrefutabilidade e a auditoria dos dados de uma eleição, como:

- lacração dos sistemas, assinatura digital e publicação do resumo digital (hash);
- auditorias pré e pós-eleição, durante o período de carga e lacração das urnas, com a participação do MP, da OAB e dos partidos políticos;
- oficialização de sistemas, com a emissão do relatório "Zerésima", (documento impresso nos equipamentos de votação (urna) e de totalização dos resultados antes do início da eleição e que comprova a inexistência de votos computados no sistema);
- tabela de correspondências esperadas entre urna e seção;
- lacres físicos;
- Votação Paralela, simulação da eleição realizada concomitantemente com a votação real dos eleitores usando um sistema informatizado de captação e contabilização de votos, com o objetivo de demonstrar o funcionamento e a segurança das urnas eletrônicas.

Vale ressaltar, também, que o Brasil não é o único país a utilizar equipamento eletrônico de votação. Segundo o IDEA (International Institute for Democracy and Electoral Assistance), instituto internacional que visa à promoção da democracia no mundo, pelo menos 25 nações empregam um sistema semelhante. Entre eles estão Canadá, França, Austrália e Índia, além de alguns estados dos Estados Unidos da América (EUA).

Ainda de acordo com o Electoral Integrity Project (Projeto de Integridade Eleitoral), trabalho de pesquisa acadêmica realizado pelas Universidade de

Harvard e Sidney, as eleições brasileiras têm índice elevado de integridade, estando à frente, na comparação mundial, de países como os EUA.

Por fim, o TSE mantém o site "Fato ou Boato" para esclarecer informações de cunho duvidoso a respeito da eleição. A série em vídeo "Minuto da Checagem" mostra os riscos de as pessoas compartilharem dados sem confirmá-los, enquanto outra chamada "Mitos Eleitorais" desconstrói supostos fatos relativos à Justiça Eleitoral.

COMBATE

Como identificar (e não compartilhar) desinformação

As eleições exigem uma tomada de decisão que terá efeitos por, no mínimo, quatro anos. Nesse contexto, evitar informações falsas transmitidas pelas redes sociais falsas é fundamental.

Listamos a seguir algumas dicas oferecidas pelo site de checagem americano PolitiFact para se prevenir contra a desinformação.

a) Não leia só o título

Uma estratégia muito utilizada pelos criadores de conteúdo falso na internet é

criar títulos bombásticos. Ler o texto completo é um passo básico para evitar compartilhar desinformação. Muitas vezes, a leitura da matéria permite concluir que os fatos descritos não correspondem ao título provocativo. É preciso, então, ler o texto completo para avaliar se existe ligação entre ele e o título.

b) Verifique o autor

É importante ver quem é o autor da matéria. Se um repórter assina o texto, há como responsabilizar o site pela qualidade da informação. Ver quem escreveu determinado texto é importante para dar credibilidade ao que está sendo veiculado. É recomendável evitar o compartilhamento de notícias caso não haja a identificação do autor.

c) Veja se conhece o site

Não deixe de olhar a página onde está a notícia. Navegar mais no site ajuda a analisar sua credibilidade.

d) Observe se o texto contém erros ortográficos

As reportagens jornalísticas, em geral, valorizam o bom vocabulário e o uso correto da gramática. Por sua vez, os sites com notícias falsas ou mensagens divulgadas pelo WhatsApp tendem a apresentar uma escrita fora do padrão, com erros de português ou quantidade exagerada de adjetivos.

e) Olhe a data de publicação

Identifique quando a notícia foi publicada. Muitas vezes, o texto está simplesmente fora de contexto. Há também notícias que, embora não sejam falsas, estão desatualizadas.

f) Saia da bolha da rede social

Para estar bem informado, o eleitor deve ler e acompanhar o noticiário não somente nas redes sociais. É preciso buscar fontes e veículos com uma trajetória de prestação de serviços de informação à comunidade. Isso evita uma visão distorcida do que está acontecendo.

Para o eleitor conhecer mais sobre o processo eletrônico de votação brasileiro e urna eletrônica, deve buscar as informações oficiais, ou seja, no site do TRE-SP www.tre-sp.jus.br ou do TSE www.tse.jus.br.

DÚVIDAS PRINCIPAIS

a) O que é desinformação?

O termo designa informações falsas ou imprecisas que, na maioria das vezes, são divulgadas pela internet, de modo rápido e eficiente. É comum falarem em fake news, mas a Justiça Eleitoral opta por utilizar o termo desinformação, uma vez que especialistas entendem que a expressão ganhou conotação pejorativa e ambígua, muitas vezes utilizada para desacreditar a imprensa.

Há divulgações por mensagens no WhatsApp, no feed de notícias do Facebook ou Twitter, de conteúdos falsos usados para influenciar opiniões e comportamentos. A vida político-partidária não está livre desse fenômeno.

Uma possível novidade para as Eleições 2020 é a propagação de "deepfakes", tecnologia que usa inteligência artificial para criar vídeos falsos, porém realistas, de pessoas fazendo coisas que nunca fizeram realmente. Efeitos especiais de computador que criam rostos e cenas no audiovisual não são algo inovador, mas a tecnologia ficou muito acessível com o "deepfake": qualquer pessoa com acesso a algoritmos e conhecimentos de deep learning, um bom processador gráfico e um amplo acervo de imagens pode criar um vídeo falso que seria convincente. Por isso, é recomendável ficar sempre atento e checar as informações propagadas.

b) Qual deve ser a conduta de uma pessoa que for vítima de uma ofensa na internet?

Recomenda-se não apagar o conteúdo e salvar os arquivos que comprovem o delito, como e-mails, capturas de tela, fotos, vídeos, links e conversas em rede social, aplicativos ou qualquer outro material. Pode-se registrar um boletim de ocorrência. A autoridade policial pode investigar o ocorrido e prestar informações ao Ministério Público, que poderá acionar o Judiciário. Pessoas e entidades privadas também podem pleitear providências na Justiça.

c) É possível identificar e responsabilizar quem cria e dissemina notícias falsas ou ofensivas?

Há previsão legal para responsabilizar quem cria e dissemina informações falsas, mas é necessário identificar a pessoa ou a empresa que a divulga. Quando a divulgação tem como alvo uma pessoa em específico, a conduta pode ser enquadrada como crime de calúnia, difamação ou injúria previstos no Código Penal e também é possível, dependendo do caso, que haja a responsabilização

civil do ofensor a pagar indenização por danos morais.

d) Como combater a desinformação em período eleitoral?

Considerando que as campanhas eleitorais se utilizam da internet para, entre outros objetivos, disseminar informações falsas ou imprecisas, a Constituição Federal, as leis e as Resoluções do TSE preveem responsabilização civil e criminal para quem descumprir as regras eleitorais.

e) De acordo com a legislação atual, compartilhar conteúdos falsos é crime? Qual a punição?

Quando uma postagem é compartilhada, cresce a visualização dela, aumentando assim seu potencial ofensivo.

O compartilhamento de notícias falsas pode configurar crimes, gerando responsabilização cível mediante pagamento por danos morais.

BOATOS

Nas eleições gerais brasileiras de 2018, houve intensa disseminação de boatos a respeito dos envolvidos no processo eleitoral. O próprio sistema eletrônico de votação foi alvo de diversos ataques.

A divulgação de boatos pode ter inúmeros autores e, como visto no capítulo anterior, é passível de condenação.

O cidadão precisa se conscientizar do problema e ter uma atuação responsável. Listamos alguns boatos que se espalharam rapidamente naquela eleição:

a) Compartilhamento de pesquisas e sondagens eleitorais não registradas no TSE:

A pessoa recebe e compartilha supostos dados de pesquisa não realizada ou então feita em desacordo com a legislação eleitoral;

b) Supostas fraudes em urnas eletrônicas:

A urna eletrônica é um equipamento eletrônico, como um computador e, dessa forma, está sujeita a falhas mecânicas, o que não corresponde de forma alguma a fraude. As falhas podem ocorrer e, para esses casos, a Justiça Eleitoral conta com suas urnas de contingência, para efetuar prontamente a substituição do equipamento. Caso haja irregularidade com alguma urna, o fato deve constar da ata, a cargo dos mesários.

Não basta alegar que houve fraude em determinada urna para que isso se torne uma verdade. Seria preciso documentar o fato, instruir o processo e, finalmente, haver decisão judicial sobre o assunto.

Contudo, até hoje nenhuma fraude foi comprovada e as urnas eletrônicas seguem sendo utilizadas por ser uma tecnologia inteiramente confiável, além de garantir o sigilo do voto do brasileiro e a rápida apuração dos resultados.

c) Declarações falsas de apoio de famosos a determinado candidato ou partido.

Aproveitar-se indevidamente da notoriedade do artista.

d) Frases tiradas de contexto.

É necessário ler o texto completo de uma notícia, para evitar a distorção das ideias.

e) Uso de tecnologias para manipular fotos, vídeos e áudios de WhatsApp.

O uso de tecnologias pode levar o cidadão a acreditar que determinada divulgação é verdadeira, mas elas podem ser muito bem feitas e criar conteúdo falso. Daí a necessidade de o receptor desse tipo de falsidade tomar as devidas precauções antes de compartilhá-la.

f) Não aparece a tecla para confirmar o voto.

A tecla “confirma” na urna eletrônica é uma tecla física, na cor verde, no canto inferior da urna eletrônica, para confirmar o voto digitado. Toda urna eletrônica apresenta a tecla.

g) Empresa venezuelana teve acesso aos códigos da urna eletrônica.

Em 2017, o TSE realizou licitação para aquisição de módulos impressores para as urnas, vencida por empresa fundada por dois venezuelanos e sediada nos EUA. Os módulos impressores apresentados pela empresa não atenderam às exigências do TSE, ocasionando a eliminação da empresa do certame.

h) Mesário pode anular voto do eleitor.

O mesário não tem meios de anular um voto. Somente o eleitor pode anular o próprio voto ao digitar um número que não corresponde a candidato ou partido político.

i) Só o Brasil, Cuba e a Venezuela utilizam urna eletrônica.

Segundo o Instituto Internacional para a Democracia e a Assistência Social (IDEA Internacional), 23 países usam urnas com tecnologia eletrônica para eleições gerais e outros 18 em pleitos regionais. Entre os países estão o Canadá, Índia e a França, além de alguns estados dos Estados Unidos da América.

j) Eleitor não consegue votar em seu candidato. Ao digitar o número, aparece a mensagem "voto nulo".

Nas Eleições 2018, foi verificado que houve engano por parte dos eleitores quanto à ordem de votação. A auditoria denominada Votação Paralela comprova em tempo real que os equipamentos utilizados no dia da eleição são íntegros.

SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO

A Justiça Eleitoral realiza uma série de procedimentos para comprovar a segurança do sistema que desenvolveu há 24 anos, em 1996.

Esses procedimentos estão mencionados no capítulo dois, mas importante detalharmos o funcionamento da Votação Paralela, que se trata de uma auditoria em tempo real com a votação dos eleitores no dia da eleição.

Na véspera do dia da eleição, o TRE-SP convida um grupo de pessoas para o preenchimento de mais de 2 mil cédulas de papel com votos nos candidatos oficiais, aqueles que de fato estão disputando o pleito.

Nas últimas eleições, o Tribunal convidou crianças e adolescentes de um grupo de escoteiros e bandeirantes de São Paulo. Em pleitos anteriores, representantes dos partidos políticos faziam esse preenchimento.

As cédulas são preenchidas com números correspondentes a candidatos registrados e votos de legenda, assim como votos nulos e brancos. Após, são guardadas em uma urna de lona lacrada na presença de auditor, Ministério Público e fiscais de partido.

Também na véspera do pleito são sorteadas, por amostragem, cinco urnas eletrônicas já prontas para serem usadas pelos eleitores. O sorteio contempla urnas de todo o Estado e os equipamentos sorteados são levados para o Tribunal Regional Eleitoral de São Paulo para a averiguação.

O juiz eleitoral da localidade sorteada substitui a urna por outra que havia sido preparada com o mesmo procedimento das originais e seria utilizada

em caso de contingência.

No dia da eleição, durante o horário da votação, ou seja, em simultâneo e em paralelo com a votação oficial, são retirados os lacres das urnas de lona e funcionários da Justiça Eleitoral digitam, em computadores e nas urnas sorteadas, os votos contidos nas cédulas de papel.

Todo o procedimento, da leitura do voto à digitação na urna, é filmado e realizado na presença de auditoria externa contratada pelo TSE, dos fiscais dos partidos políticos, da imprensa e de quaisquer outros interessados.

Às 17 horas é encerrada a votação e os votos registrados nas urnas são apurados. O resultado verificado na totalização dos computadores deve coincidir com o resultado das respectivas urnas eletrônicas, a fim de comprovar que não há adulteração, subtração ou acréscimos na votação das urnas eletrônicas.

NORMAS JURÍDICAS

- Constituição Federal: artigos 5º, incisos II, IV, IX, XIV e XXXVI; e 220, caput, parágrafos 1º e 2º
- Lei das Eleições (Lei nº 9.504/97): artigos 57 e 58
- Lei de Inelegibilidade (Lei Complementar nº 64/1990): artigo 22 e incisos
- Lei 12.965/14: Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil – artigo 19
- Portaria TSE 949/2017: Conselho Consultivo sobre Internet e Eleições
- Resolução TSE nº 23.551/2017 – disciplinou a Propaganda Eleitoral nas Eleições 2018 – artigo 22 e parágrafos
- Resolução TSE nº 23.610/2019 – Dispõe sobre Propaganda Eleitoral nas Eleições 2020 – artigo 9º trata da desinformação na propaganda eleitoral

REFERÊNCIAS

Globo.com : Fato ou Fake? Saiba como identificar se um conteúdo é falso. Disponível em https://g1.globo.com/fato-ou-fake/noticia/2018/09/25/fato-ou-fake-saiba-como-identificar-se-um-conteudo-e-falso.ghtml

TSE: Programa de enfrentamento à Desinformação com foco nas Eleições 2020;

El País: Como reconhecer uma notícia falsa para não compartilhar mentiras. Disponível em: https://brasil.elpais.com/brasil/2018/09/20/politica/1537467412_871279.html;

Brasil Escola: O que são Fake News? Disponível em: https://brasilescola.uol.com.br/curiosidades/o-que-sao-fake-news.htm

IDEA: Use of E-Voting Around the World. Disponível em: <https://www.idea.int/news-media/media/use-e-voting-around-world>

TSE: Fato ou Boato? Esclarecimento Sobre Informações Falsas. Disponível em: <http://www.justicaeleitoral.jus.br/fato-ou-boato/>

COORDENAÇÃO EDITORIAL:
Marina Mello Rocha Campos

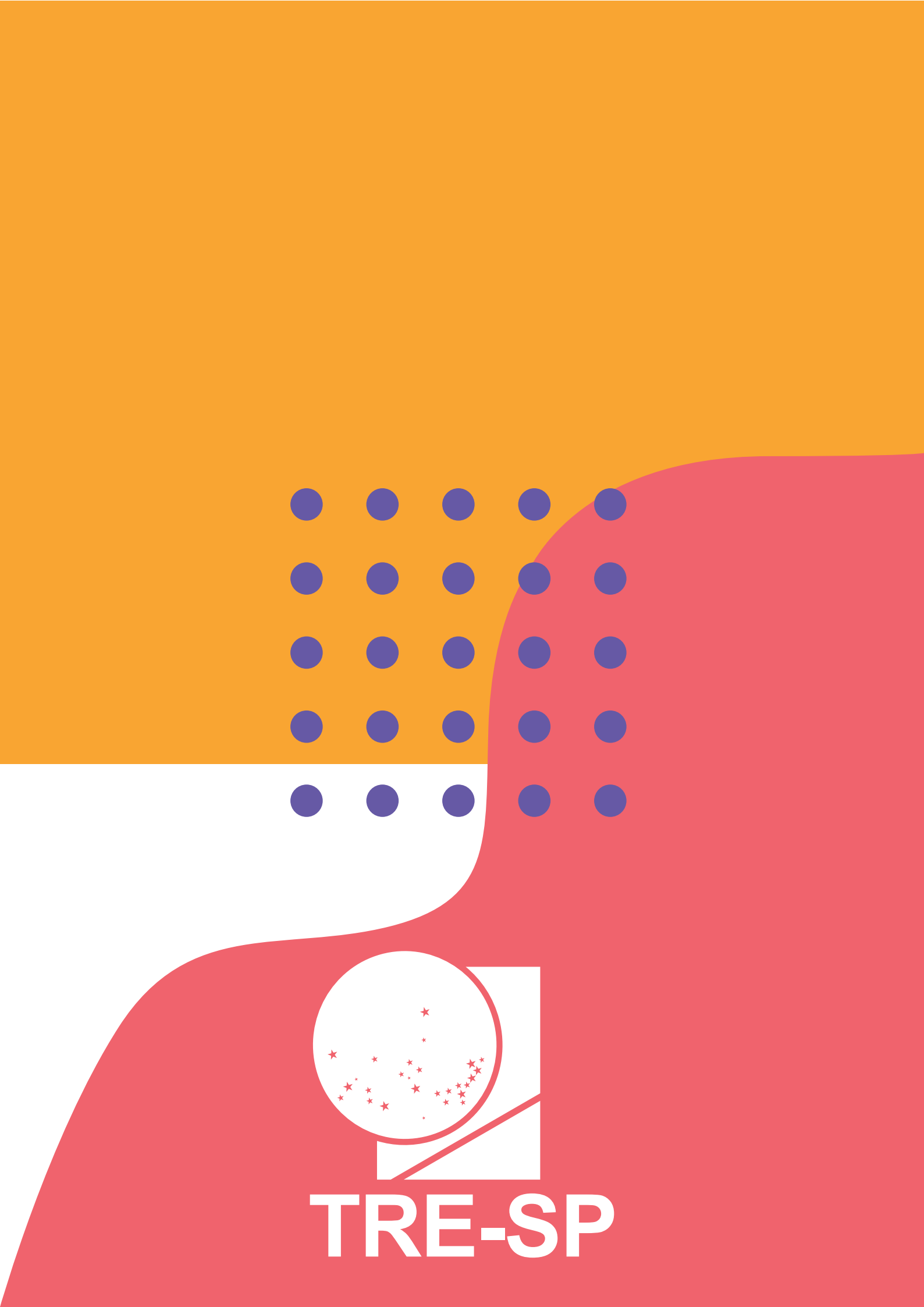
REDAÇÃO:
Henrique Marcelo Moretti Filho
Imad Ali Nasser

REVISÃO:
Flávia Andréia dos Santos
Marina Mello Rocha Campos
Nadhia Auxiliadora Mesquita Pinheiro Nakaya
Vitor Amaral Magno da Silva

PROJETO GRÁFICO:
Ian Duarte Augusto
Marcelo Lessi de Mello
Melissa Rodrigues Costa Passos

FOTOGRAFIA:
Banco de imagens da CCS

PUBLICAÇÃO:
Portal do TRE- www.tre-sp.jus.br


TRE-SP