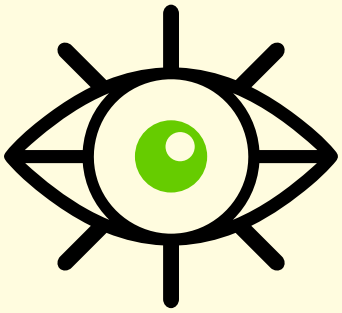
ELEIÇÕES, INTERNET E DIREITOS

Contribuições da Coalizão Direitos na Rede ao processo eleitoral de 2020



COALIZÃO
DIREITOS NA REDE

DADOS PESSOAIS • ACESSO À INTERNET
LIBERDADE DE EXPRESSÃO • PRIVACIDADE E VIGILÂNCIA

Realização: Coalizão Direitos na Rede (CDR)

Secretaria Executiva: Fabrício Solagna

Comunicação: Ênio Lourenço

Assessoria de imprensa: Adriana Veloso

Pesquisa e redação: Evorah Cardoso, Francisco Brito Cruz, Heloísa Massaro, Joana Varon e Olívia Bandeira

Edição: Bia Barbosa

Diagramação: Leo Garbin

Força Tarefa da CDR para as Eleições 2020

Bia Barbosa, Flávia Lefèvre, Maria Mello e Olivia Bandeira – Intervozes

Bruna Santos

Evorah Cardoso e Maria Luiza Freire Mercês – #MeRepresenta

Francisco Brito Cruz – InternetLab

Gustavo Ramos Rodrigues – Instituto de Referência em Internet e Sociedade (IRIS)

Janaína Spode – Casa de Cultura Digital de Porto Alegre

Joana Varon – Coding Rights

Josué Gomes – Internet Sem Fronteiras

Mariana Canto e Raquel Saraiva – IPRec

Taís Ladeira – Amarc Brasil

Apoio: Fundação Heinrich Böll

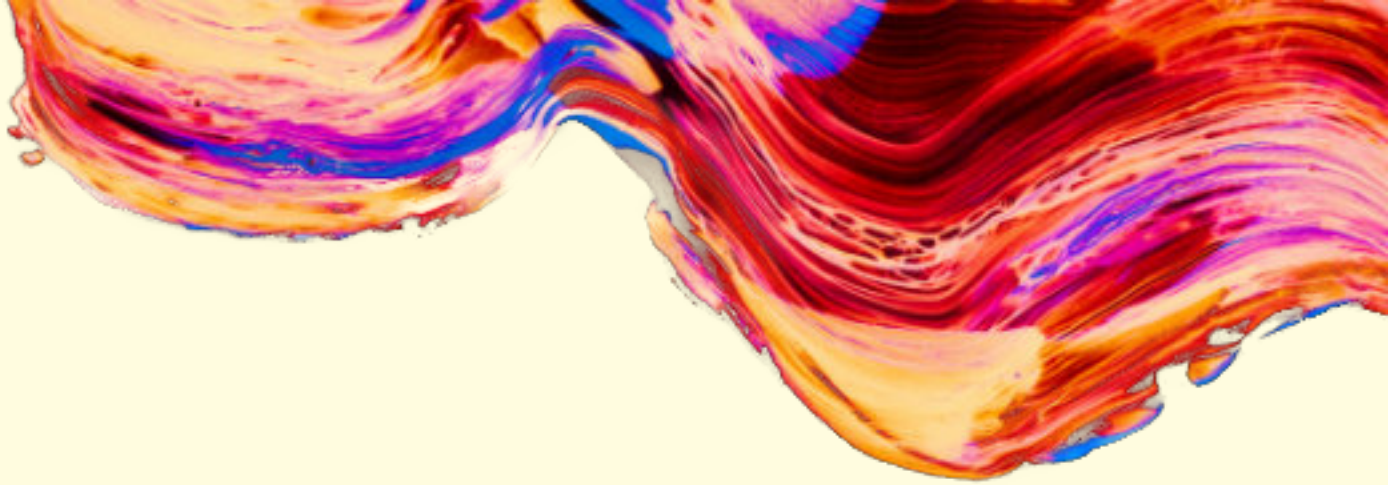
@cdr_br

/direitosnarede

@direitosnarede

medium.com/@cdr_br

direitosnarede.org.br



SUMÁRIO

1. CONTEXTO

As eleições deste ano acontecerão em um contexto de pandemia, em que o isolamento social torna ainda mais relevante o papel da Internet para a informação dos eleitores, formação da chamada opinião pública e realização das campanhas. Parte significativa do debate eleitoral será travada em poucas plataformas digitais, que suportam conteúdos gerados por terceiros, cujo negócio está assentado na coleta e tratamento de dados pessoais para o direcionamento da informação e da publicidade, como o *Facebook*, o *Twitter* e o *Instagram*.

No Brasil, onde o acesso à internet é desigual, predominando nas classes C, D e E o uso limitado da rede em poucas aplicações, também ganhará mais relevância o compartilhamento de conteúdos por aplicativos de mensageria instantânea, como o *WhatsApp* e o *Telegram*, nos quais as fronteiras entre sistemas de comunicação privada e de disseminação pública não estão muito definidas. Este contexto traz desafios novos e bastante concretos não apenas para as milhares de candidaturas que disputarão o voto dos eleitores, mas para os operadores do sistema de Justiça Eleitoral, para os partidos políticos e para o setor privado – em especial, para as plataformas digitais.

Um dos temas que tem gerado maior preocupação gira em torno da produção intencional de desinformação e seus impactos no jogo eleitoral. Se este já foi um problema detectado nas eleições majoritárias de 2014 e de 2018, torna-se uma desafio ainda maior num cenário de um pleito descentralizado em mais de cinco mil municípios, o que dificulta inclusive a fiscalização por parte do sistema de Justiça. Proteger o processo eleitoral sem ferir os direitos à informação e à liberdade de expressão dos usuários é uma questão que está no centro da discussão política nacional.

A pressão por respostas às chamadas *fake news* fez com que uma série de medidas venham sendo adotadas pelas plataformas. Nas eleições de 2018, os esforços das empresas centraram-se sobretudo na parceria com agências de checagem para a classificação de notícias em escalas entre verdadeiro e falso e a moderação dos conteúdos a partir dessa classificação. Algumas medidas adotadas a partir da classificação foram: redução do alcance de notícias consideradas falsas

(*Facebook* e *Google*), alerta aos usuários sobre a classificação das notícias (*Facebook*) ou sobre se a fonte era originária de terceiros (*WhatsApp*) e mesmo exclusão de páginas e perfis considerados "mal-intencionados" ou disseminadores de *spam* (*Facebook* e *Twitter*).

Os acordos, entretanto, não impediram a disseminação de notícias falsas. Balanço divulgado no dia 31 de outubro pela "Aos Fatos" mostra que a agência "desmentiu" 113 "boatos" durante as eleições, número pequeno comparado à quantidade de desinformação que circulou na rede. Além disso, o alcance da verificação foi bem menor do que o das notícias originais. No *WhatsApp*, o volume da disseminação é impossível de ser acompanhado, devido ao caráter fechado da rede. Mesmo quando checadas, muitas das informações falsas continuaram sendo disseminadas nas redes sociais, diante da omissão da Justiça Eleitoral e das plataformas digitais. O caso mais emblemático foi o do "kit gay" que, mesmo classificado como falso e proibido pelo TSE, voltou a ser veiculado pela campanha de Bolsonaro.

O *Twitter* anunciou que não mais aceitará publicidade política de qualquer tipo em sua plataforma. O argumento é que os anúncios políticos da Internet utilizam otimização baseada em aprendizado de máquina de mensagens e segmentação múltipla, além de informações enganosas não verificadas e as *deep fakes*, com velocidade crescente e grande escala. Outras plataformas, entretanto, não adotaram a mesma medida.

Nas eleições, o fenômeno da desinformação se conecta em grande medida com o crescimento da violência política e do discurso de ódio. Segundo dados da ONG *SaferNet*, o contexto eleitoral está relacionado a uma explosão de denúncias de racismo, xenofobia, apologia e incitação a crimes contra a vida na internet. Desde o período eleitoral de 2018, a enúncias recebi das também pela *SaferNet* cresceram 21,27% em abril de 2020, em relação ao mesmo período no ano passado – e isso deve se agravar em relação a mulheres que ocupam a esfera pública e que disputem as eleições. O avanço da violência política de gênero vem sendo documentado no Brasil e no mundo, com normatização recente na América Latina e o reconhecimento de que a prática se dá, em parte, por meio da internet.

A pesquisa *Perfil das Prefeitas no Brasil: mandato 2017-2020*, que entrevistou 314 mulheres eleitas para as administrações locais, aponta que a segunda maior dificuldade de acesso e permanência de mulheres na política é o assédio e as violências simbólicas no espaço político. Cerca de 53% delas afirmaram ter sofrido assédio ou violência política. Já o estudo *Eleitas: mulheres na política*, que entrevistou 96 mulheres na América Latina, aponta que 99% das entrevistadas foram vítimas de algum tipo de violência por ocuparem e disputarem espaço político.

Nas eleições de 2018, a iniciativa brasileira *Tretaqui.org* desenvolveu um canal para o recebimento de denúncias sobre candidaturas que foram atacadas ou que fizeram uso de discurso de ódio como estratégia de marketing político (apologia e incitação a crimes contra a vida, discriminação contra a mulher, LGBTfobia, incitação à violência física, racismo, invasão de conta de email ou redes sociais e intolerância religiosa). Foram coletadas 564 denúncias de links (a maioria de posts em redes sociais e algumas notícias) que indicavam violações, principalmente contra candidaturas que atacavam grupos da população (mulheres, especialmente

feministas, e LGBTs), além de apologia e incitação à violência (especialmente contra criminosos). No *Relatório Descritivo de Denúncias da Plataforma Tretaqui.org: Contribuição para a Missão de Observação Eleitoral da OEA (2018)*, é possível observar que boa parte das denúncias recebidas foram contra candidatos vinculados a um mesmo partido (PSL).

Vale reforçar que o discurso de ódio contra candidaturas é um ato de violência, cuja utilização em contextos eleitorais tem o objetivo exclusivo de silenciar a expressão de candidaturas representativas de grupos minoritários, servindo apenas para o acirramento do debate político e a polarização no país, além de fomentar a violência dentro e fora dos pleitos eleitorais. Praticado por candidaturas, ele revela sua instrumentalização como ferramenta de marketing político eleitoral, adotada não apenas por campanhas isoladamente, mas também por partidos, valendo-se principalmente das redes sociais para sua propagação.

O direcionamento e articulação de tais práticas de violência conta com uma ferramenta importante: o uso de dados pessoais para a produção e direcionamento de conteúdos. O aprimoramento das capacidades tecnológicas de coleta, processamento e armazenamento de dados, combinado com sua incorporação em ferramentas de marketing digital, favoreceu a crescente adoção por campanhas eleitorais de estratégias de marketing digital que se valem do uso de dados pessoais de eleitores. Adotando muitas vezes ferramentas desenvolvidas no âmbito do marketing comercial para convencer consumidores a adquirir produtos e serviços, campanhas passam a se valer de bancos de dados e ferramentas de coleta e análise de dados como parte de suas estratégias para conquistar eleitores.

Pesquisas recentes revelam como a adoção de uma diversidade de técnicas e ferramentas que se valem da coleta, processamento, análise e armazenamento de dados pessoais vem se disseminando em processos eleitorais ao redor do mundo. Recursos valiosos para campanhas político-eleitorais, dados pessoais podem auxiliar campanhas a conhecer melhor seu potencial eleitorado, definir narrativas e mensagens, direcionar e microdirecionar anúncios políticos, enviar propaganda eleitoral e material de campanha e se comunicar com eleitores.

Pesquisa da Coding Rights em parceria com a *Tactical Tech* revelou todo um mercado de *data brokers* e empresas de marketing digital que oferecem serviços para campanhas baseados na construção de inteligência sobre eleitores, na segmentação desses eleitores em grupos e no micro direcionamento de conteúdos, a partir de grandes bancos de dados pessoais formados a partir de bancos de dados públicos, da análise de mídias sociais, de pesquisas internas e de outros bancos de dados adquiridos de terceiros ou recebidos de clientes. No caso das eleições de 2018, os próprios *disparos em massa* em aplicativos de mensagens privadas nunca teriam sido possíveis sem o tratamento de números de telefone dos destinatários dos disparos.

Vale ressaltar que a formação de bancos de dados com informações de eleitores e apoiadores e a busca por conhecer melhor o eleitorado em potencial não são práticas novas em campanhas políticas. O que é novo é a incorporação de novas capacidades tecnológicas que aumentam significativamente as possibilidades de coleta e análise de dados não só em termos quantitativos mas, principalmente, qualitativos.

Por um lado, a possibilidade de uma comunicação mais direcionada pode aproximar a campanha do eleitor, estabelecendo uma comunicação mais relevante para aquele eleitor e favorecendo seu engajamento no debate público. A possibilidade de uma comunicação mais direcionada que atinja que uma parcela do eleitorado que tenha maior afinidade com o projeto político de determinado candidato já chegou a ser até uma promessa de maior eficiência na comunicação para campanhas menores com recursos limitados. No entanto, por outro lado, o uso indiscriminado de dados pessoais e a adoção de estratégias de marketing que tratam o eleitor como mero consumidor colocam uma série de novos desafios e riscos a direitos fundamentais e à integridade de processos eleitorais.

Ameaças à privacidade e à proteção de dados pessoais de eleitores somam-se a riscos de violações à autonomia do eleitor de se informar e decidir. Ao conhecer melhor aquele eleitor ou aquele grupo de eleitores, campanhas passam a ter maior poder de persuasão e até de manipulação sobre esse eleitorado. Da mesma forma, a possibilidade de direcionamento e microdirecionamento pode favorecer divisões no eleitorado e no debate público, além de reduzir a transparência sobre a totalidade das campanhas, diante da possibilidade de que mensagens contraditórias sejam veiculadas paralelamente a públicos distintos. Nas eleições de 2020, este cenário se torna ainda mais complicado, diante da recém entrada em vigor da Lei Geral de Proteção de Dados e da ausência de uma ponte entre o regime de proteção de dados e a legislação eleitoral.

2. LEGISLAÇÃO EM VIGOR: PROTEÇÃO DE DIREITOS NA PRÁTICA

Cabe lembrar que parte dos problemas elencados acima já têm tratamento no sistema jurídico brasileiro, especialmente no eleitoral. Naturalmente, trata-se de um sistema em constante atualização, por meio de reformas legislativas e de resoluções do Tribunal Superior Eleitoral, que tem o poder de detalhar como devem ser interpretadas e aplicadas as regras das eleições. E cuja aplicação depende da conscientização, capacitação e comprometimento com direitos fundamentais por parte de seus operadores - advogados, promotores e juízes. Mas o país já conta com leis aplicáveis à desinformação, à violência política e discurso de ódio e a questões de proteção de dados e proteção da privacidade no processo eleitoral. Destacamos as seguintes:

Código Eleitoral e Lei das Eleições

O Código Eleitoral e a Lei das Eleições estabelecem os principais limites da propaganda e de toda a comunicação sobre o processo eleitoral e os termos de sua fiscalização, o que os torna peças legislativas que merecem contínua atenção. Entre as peculiaridades do sistema brasileiro, está o fato de que não há definição do que é *propaganda eleitoral*, o que torna a atividade de aplicação de uma série de regras extremamente desafiadora. A Coalizão Direitos na Rede se preocupa com o tênue equilíbrio de direitos que advém desta situação.

Apesar de concentrar disposições importantes, como a lista de crimes eleitorais aplicáveis, o Código Eleitoral (Lei 4.737/1965) é uma legislação antiga, que conserva pontos herdados do período da Ditadura Militar - inclusive, de suas leis de segurança nacional. Desta maneira, é uma lei importante, mas que carece de uma aplicação consciente e compatibilizada com os direitos conquistados posteriormente na Constituição Federal. Um de seus destaques é o rol de crimes contra a honra eleitorais - difamação, injúria, calúnia e denunciação caluniosa eleitoral (artigos 324, 325, 326 e 326-A) -, que se somam aos crimes contra honra como pontos que podem

ser acionados em casos que envolvem assassinatos de reputação ou de violência política, por exemplo. Outro é o crime que proíbe a divulgação de "fatos sabidamente inverídicos" capazes de exercer influência no eleitorado (art. 323).

A Lei das Eleições (Lei 9.504/1997), por sua vez, concentra os principais dispositivos que regulam a propaganda eleitoral na internet (art. 57 e subsequentes), o que a torna essencial para a garantia de uma série de direitos de usuários da rede durante as eleições. Construída após sucessivas reformas nas últimas décadas, ela estabelece, por exemplo, que qualquer cidadão pode se manifestar livremente na internet no período, assegurando o direito de resposta (57-D). É ela também que traz alguma regulação sobre o uso de cadastros eletrônicos por campanha, vedando sua venda ou a doação por uma série de autores (57-E), regra que ganha especial importância em campanhas movidas por dados pessoais.

Legislação penal

A utilização de tais dispositivos penais é tema de especial sensibilidade para a Coalizão Direitos na Rede, devendo ser reservada aos casos gravíssimos e sem possibilidade de tratamento em outra esfera. Porém, casos que envolvem violência política, discurso de ódio ou mesmo desinformação podem ganhar importância na esfera penal, dependendo das circunstâncias. Em razão disso, é fundamental assegurar a aplicação equilibrada e sempre de acordo com direitos dos usuários de dispositivos como os crimes contra honra, injúria racial ou de proteção à ordem pública, como constantes no Código Penal e na Lei de Contravenções Penais. Como a violência política e a violação da privacidade podem se originar a partir da invasão de dispositivos informáticos, regras de igual importância são aquelas trazidas ainda pela Lei Carolina Dieckmann (Lei 12.737/2012), que reformou o Código Penal.

Leis Maria da Penha, Lola e Antirracismo

Se por um lado a legislação penal é sempre lembrada no combate à violações de direitos, por outro leis como a Lei Maria da Penha (Lei 11.340/2006), a Lei Lola (Lei 13.642/2018) e a Lei Antirracismo (Lei 7.716/1989) por vezes passam ao largo da importância que de fato têm para o enfrentamento da violência política - em especial de suas modalidades que carregam recortes de gênero, raça, orientação sexual e outros marcadores. Necessário recordar que está garantida a aplicação da Lei Antirracismo para casos de LGBTfobia, conforme decisão do Supremo Tribunal Federal na ADO 26 e no MI 4733. Preocupada com o efeito que as mais diversas formas de preconceito, discriminação e violência se manifestam no processo político, a Coalizão Direitos na Rede relembra que tais normas devem estar ao lado de candidatas, candidatos, cidadãs e cidadãos durante o processo eleitoral.

Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados Pessoais (Lei 13.718/2018) traz todo um regramento para o tratamento de dados que pode incidir não só sobre seu uso por campanhas políticas, mas sobre toda uma gama de atores envolvidos com marketing político digital, como agências de marketing e data brokers. O artigo 5º da Lei, por exemplo, traz definições de dados pessoal e dado pessoal sensível, essenciais pelo fato de que informações sobre opinião política se enquadram nessa categoria. O

artigo 20, por sua vez, fala da revisão de decisões tomadas por sistemas automatizados, que, como mostramos, é fundamental em um contexto em que a análise e desenho de perfis e comportamentos estão entre os principais mecanismos usamos para de direcionamento de desinformação.

Com a entrada da LGPD em vigor em agosto de 2020, dois pontos da Lei em especial requerem atenção imediata de campanhas e seus prestadores de serviço, bem como da Justiça Eleitoral: as bases legais para tratamento de dados e os princípios da lei. No primeiro caso, destacam-se, para o cenário eleitoral, a hipótese de tratamento mediante consentimento do titular e a hipótese de tratamento quando necessário para atender o legítimo interesse do controlador. Nesta última hipótese, a análise deve ser feita caso a caso, considerando a legitimidade do interesse, a necessidade e adequação do tratamento, a legítima expectativa do titular quanto ao tratamento de seus dados e as salvaguardas adotadas para garantir transparência e segurança. Nenhuma das duas hipóteses pode ser considerada uma carta branca para realização de tratamentos de dados pessoais.

Os princípios da LGPD (Art. 6º) também devem ser vistos como atenção. Diante da decisão do STF sobre o caso IBGE/Teles, que respaldou a lei enquanto norte interpretativo, indicando uma aplicação principiológica da lei mesmo que ainda não vigente, os princípios da LGPD ganharam relevância especial para a proteção de dados pessoais nas eleições deste ano, sobretudo os princípios da finalidade, da adequação, da necessidade, da transparência e da prevenção que podem oferecer parâmetros para o tratamento de dados pessoais por campanhas eleitorais.

Marco Civil da Internet

O Marco Civil também detém mecanismos importantes a serem considerados no processo eleitoral. Sua compatibilização com a legislação eleitoral é fundamental para garantia da liberdade de expressão na rede, por desincentivar que as plataformas façam controle prévio de conteúdo de seus usuários que queiram se manifestar politicamente. Ao mesmo tempo, a Lei possui mecanismos para remoção de conteúdo íntimo, protegendo candidatas e candidatos de exposição de sua intimidade (mais um vetor de violência política), e regras relativas à coleta e tratamento de dados na internet. Neste sentido, em um período de vigência recente da LGPD, o Marco Civil deve ser considerado um respaldo adicional para determinar que campanhas e seus fornecedores respeitem normas de garantia da privacidade dos eleitores.

Resoluções do TSE

Por fim, as resoluções do TSE, atualizadas sempre antes de cada processo eleitoral, são o conjunto de normas mais concreto aplicável ao período. De uma maneira geral, as resoluções uniformizam o entendimento e a interpretação sobre a Lei Eleitoral e o Código Eleitoral, inclusive na sua relação com outras leis, como a LGPD.

A Resolução nº 23.610, de 13.12.2019, que regulamenta os assuntos de propaganda eleitoral, concentra uma série de interpretações relevantes sobre os temas acima, avançando em relação às resoluções anteriores em alguns aspectos.

Entre os passos dados pelo TSE em 2019, destaca-se a obrigação do candidato, partido ou coligação de verificar a fidedignidade de informações veiculadas em seus canais de propaganda. Estão entre estas novidades também os dispositivos de regulamentação do artigo 57-E da Lei Eleitoral, que passaram a citar a LGPD (art. 41) e avançaram para vedar a doação empresarial de bancos de dados pessoais (art. 31), bem como disparos em massa em aplicativos de mensagens feitos sem anuência dos destinatários (art. 34).

Além das novidades incorporadas em 2019, a resolução reforça pontos importantes que vem se sedimentando na Justiça Eleitoral, como a vedação de propaganda eleitoral que "veicule preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação" ou que incite atentado contra pessoa (art. 22). Neste sentido, a Coalizão Direitos na Rede reforça a importância de que a Justiça Eleitoral aplique cada um destes dispositivos de forma atenta e protetiva aos direitos de usuários de internet, garantindo um processo eleitoral democraticamente vigoroso e no qual a participação cidadã possa ocorrer livre, sem coação ou violência e desembaraçada de tentativas de manipulação a partir de dados pessoais.

3. DESAFIOS NO PROCESSO ELEITORAL

Para que haja um ambiente protetivo aos dados pessoais de cidadãos durante processos eleitorais, a legislação eleitoral e o regime de proteção de dados precisam estar em harmonia. Ao mesmo tempo em que é necessário garantir um cenário protetivo à privacidade, aos dados pessoais e à autonomia do eleitor, que fomente um debate público autêntico e democrático, sem que isso implique em restrições excessivas que impeçam que candidatos se comuniquem com eleitores, é importante construir um diálogo entre a racionalidade da atuação da Justiça Eleitoral com a racionalidade de um regime de proteção de dados.

Entre estruturas antigas que precisam ser retomadas e novas regras que necessitam efetividade, ainda existem inúmeras lacunas e uma ponte a ntes em favor de candidatos, partidos e coligações.

Em paralelo, regras já consolidadas na Lei das Eleições e no Marco Civil da Internet e avanços na redação de dispositivos trazidos pela Resolução 23.610/19 desenham um quadro normativo que garante um grau significativo de tutela sobre os dados pessoais de eleitores. Desde o Marco Civil, já vale a regra sobre a necessidade de obtenção do consentimento para o tratamento de dados pessoais na internet, bem como obrigações de transparência e direitos dos usuários. A Justiça Eleitoral e o Ministério Público devem estar atentos ao cumprimento de tais dispositivos, delimitando a área saudável da competição entre as candidaturas e coibindo abusos que ameacem a igualdade de chances ou direitos fundamentais. O que se torna ainda mais relevante no caso de candidatos que desenvolvam estratégias a partir de websites e aplicativos próprios.

Normas e limitações para o tratamento de dados pessoais também devem ter impacto sobre a disseminação e o direcionamento de desinformação no processo eleitoral. Entretanto, os desafios neste campo são maiores. Está vigente no Congresso Nacional a Comissão Parlamentar Mista de Inquérito (CPMI) das Fake News, que tem a prerrogativa de investigar a criação de perfis falsos e ataques cibernéticos para influenciar as eleições de 2018. O trabalho da CPMI, no entanto, não foi finalizado por causa da pandemia, que limitou as atividades parlamentares ao essencial, e trará poucas contribuições a serem

incorporadas pela Justiça Eleitoral e partidos políticos já no processo munici nas eleições de 2018, cabendo um esforço institucional mais sistemático e articulados e de proteção de candidaturas que garantam uma maior representatividade e participação de grupos marginalizados no debate político brasileiro. O país está longe do desenvolvimento de arranjos legais, de mecanismos institucionais e de novos padrões de regulação que permitam a implementação de estratégias coordenadas e contínuas para garantir o livre exercício da vida política pelos diversos grupos que formam a sociedade brasileira.

Neste contexto, diversos desafios estão colocados, como o risco de que medidas focadas em candidatos/candidaturas, seja para mitigar violência política ou monitorar propaganda eleitoral, não afetem toda uma rede organizada de disseminação de diferentes atos de violência política. Atualmente, as soluções colocadas raramente consideram que o uso ou apropriação de tecnologias por milícias digitais (roubos de conta, ataques em massa, manipulação de algoritmo, uso de robôs etc) resulta, mesmo que momentaneamente, no silenciamento de vozes dissidentes ou de candidaturas e apoio a candidaturas que representam populações já vulnerabilizadas. Enquanto que o inverso, ou seja, silenciamento dessa rede articulada, é mais difícil de ocorrer, também porque parte dessa rede se utiliza de táticas que tangenciam o que é permitido na lei e nos termos de uso das plataformas.

As recorrentes ameaças à liberdade de expressão e direitos políticos de grupos e candidaturas marginalizadas decorrentes da disseminação do discurso de ódio como ferramenta política não podem ser institucionalizadas no país, sob pena de tornar o acesso à política e a cargos eletivos ainda mais restritivo para vozes de mulheres, negras, LGBTQ+ e de outros grupos que, apesar de numerosos na população, ainda representam uma pequena parcela dos nossos representantes políticos.

4. RECOMENDAÇÕES PARA AS ELEIÇÕES 2020

Justiça Eleitoral e Ministério Público Eleitoral

Combate à desinformação

- Avançar na identificação e punição das empresas que disparam mensagens em massa a partir de sistemas automatizados, efetivando processos de investigação e responsabilização das fábricas de desinformação durante a campanha eleitoral.

- Considerar, em casos de direito de resposta, o alcance e a velocidade da publicação do conteúdo que motivou o pedido de reparação. A disseminação das mensagens de desmentido ou esclarecimento deve chegar aos usuários atingidos pelos conteúdos enganosos na mesma velocidade ou até mesmo em rapidez maior em casos específicos (como na reta final de eleições).

- Realizar formações para que os operadores do sistema de Justiça Eleitoral empreguem a legislação já existente no enfrentamento à desinformação durante as eleições, de maneira a ampliar a responsabilização de candidaturas e partidos pelos conteúdos eleitorais que publicam.

Enfrentamento ao discurso de ódio e à violência política

- Monitorar se recurso público para campanhas eleitorais está sendo utilizado para práticas de discurso de ódio e outras formas de violência política.

- Adotar medidas para promover que as redes sociais não violem os direitos das mulheres, a imagem e privacidade das mulheres que participam da vida pública e combatam os conteúdos que reforçam, justificam ou toleram a violência contra as mulheres na vida política, de acordo com o artigo 15 da "Ley Modelo Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres en la Vida Política", elaborada pela OEA em 2017.

- Desenvolver campanhas de informação, com canais de denúncia, sobre violência política e seu uso como marketing político.

- Responsabilizar candidaturas, incluindo com a impugnação de seus registros, em caso de prática sistemática de crimes como racismo e LGBTfobia praticados por campanhas eleitorais e seus apoiadores diretos.

Proteção de dados pessoais

- Orientar candidaturas sobre a entrada em vigor da LGPD e sobre as bases legais para tratamento de dados durante a campanha, incluindo a utilização de emails por candidatos/as sem consentimento prévio dos destinatários.

- Fiscalizar e aplicar uma interpretação da Lei das Eleições alinhada com a LGPD e com o Marco Civil da Internet, coibindo práticas abusivas em relação à privacidade – como doação, cessão e venda de bancos de dados pessoais a candidaturas sem a devida base legal.

- Promover a fiscalização e devida aplicação do art. 57-E das Lei das Eleições de acordo com a redação do art. 31 da Resolução 23.610/19 e os princípios da LGPD.

- Promover diálogo e debate junto ao Ministério Público Eleitoral para a elaboração de um argumento comum pela tutela ou limitação de uso dos dados pessoais nas eleições.

- Realizar capacitações e treinamentos em proteção de dados pessoais para servidores do sistema de Justiça, com vistas ao devido cumprimento da Resolução 23.610/19.

- Fixar regras de transparência para o impulsionamento de anúncios políticos durante a campanha eleitoral.

ANATEL

Combate à desinformação

- Garantir espaços para acesso público à internet com informações relevantes sobre as eleições, sobretudo em localidades onde o acesso é precário ou inexistente (praça do eleitor).

- Vedar, ao menos durante a campanha eleitoral, que as empresas de telecomunicações bloqueiem a navegação dos usuários após o fim das franquias de dados, permitindo às operadoras do Serviço Móvel Pessoal e do Serviço de Comunicação Multimídia apenas a redução da velocidade da navegação, sem inviabilização do direito de acesso à Internet.

Candidaturas, partidos, campanhas políticas e advogados eleitorais

Combate à desinformação

- Incentivar a checagem de informações disseminadas por seus partidários e apoiadores e orientá-los sobre o que fazer em caso de identificação de distribuição deliberada de desinformação.

- Realizar formações sobre o tema para candidatos, a partir da ideia de que uma boa forma de combate à desinformação é a produção e disseminação de informação confiável.

Proteção de dados pessoais

- Fomentar a realização de campanhas político-eleitorais em conformidade com a Lei Geral de Proteção de Dados Pessoais e com as garantias do Marco Civil da Internet, sobretudo na uso de ferramentas de marketing digital.

- Promover a conscientização a respeito da necessidade de garantias à proteção de dados pessoais dos eleitores durante a campanhas eleitorais.

- Promover transparência sobre práticas de uso de dados pessoais, garantindo ao eleitor informações claras sobre dados coletados, finalidade do tratamento, e mecanismos de descadastramento.

- Promover diálogos e debates com advogados eleitorais para a elaboração de um argumento comum pela tutela ou limitação de uso dos dados pessoais nas eleições.

Plataformas digitais

Combate à desinformação

- Disponibilizar ao TSE, durante o período eleitoral, dados acerca de publicações de grande alcance, mesmo as não impulsionadas, que citem candidatos, coligações e partidos, de forma que o órgão proativamente analise a necessidade de adoção de medidas como direitos de resposta ou restrições ao alcance de determinados conteúdos.

- Dar transparência aos critérios utilizados pelos algoritmos para a exibição ou direcionamento de conteúdos, explicitando, se possível, seus efeitos para os usuários.

- Fornecer aos usuários mecanismos de gestão de conteúdo que permitam que cada um - e não a plataforma - decida de maneira autônoma o que quer receber e o que deve ser priorizado em termos de visualização nas redes sociais. Acordos comerciais que interferem na exibição dos conteúdos devem ser informados de forma visível junto aos conteúdos.

- Apoiar iniciativas de educação midiática durante o período eleitoral.

- Publicar, de maneira periódica, em todo o período eleitoral, relatórios de transparência sobre remoção de conteúdos, classificados de acordo com a razão de remoção, e sobre denúncias recebidas contra perfis das candidaturas nas respectivas redes sociais.

- Remover contas automatizadas não identificadas como tal, dando transparência a tal medida.

- Realizar parceria com os agentes do sistema de Justiça Eleitoral para envio rápido de denúncias eleitorais e de relatórios de transparência.

Enfrentamento ao discurso de ódio e à violência política

- Implantar mecanismos específicos para recebimento de denúncia contra violência política em contexto eleitoral, particularmente violência de gênero e suas interseccionalidades. Em caso de adoção de medidas de remoção de conteúdo, assegurar o devido processo dentro da plataforma, garantindo o direito ao contraditório.

- Incluir em seus termos de uso a vedação à discriminação contra mulheres e à violência política contra elas, de acordo com a recomendação da *Declaración sobre la Violencia y el Acoso Políticos contra las Mujeres" (2015)*, da Convenção de Belém do Pará, adotada pela Organização dos Estados Americanos (OEA) e ratificada pelo Brasil.

- Adotar medidas de transparência imediata acerca de conteúdos patrocinados e impulsionado com fins de propaganda eleitoral, incluindo informações sobre os anunciantes, o valor pago, os parâmetros de direcionamento contratados, e a audiência atingida, garantindo respeito e conformidade às regras e princípios estabelecidas pela Lei n. 13.709/2018.

- Vedar a utilização de dados sensíveis como origem racial ou étnica, convicções religiosas, filiação a sindicatos ou organizações de caráter religioso, dados referentes à saúde ou à vida sexual para o direcionamento de propaganda eleitoral.

- Promover maior transparência sobre práticas de campanhas político-eleitorais que envolvam a contratação de empresas corretoras de dados, com informações sobre as empresas contratadas, as bases de dados utilizadas e o período de guarda desses dados.

- No caso dos serviços de mensageria privada, ajuizar demandas em face de empresas de disparo em massa, cujas práticas estão vedadas pela legislação eleitoral.

Eleitores/as

- Realizar denúncias às plataformas e agentes do sistema de Justiça Eleitoral diante da constatação de ilegalidades e crimes relacionados a práticas de desinformação, discurso de ódio, violência política online e violação à proteção de dados pessoais.

- Cobrar de partidos e candidaturas o respeito a direitos fundamentais ao longo do processo político eleitoral.

- Se engajar na campanha ***Seus Dados São Você***, promovendo conscientização e sensibilização a respeito da importância da proteção de dados pessoais em contextos eleitorais.

- Acompanhar e contribuir com esforços de registro e categorização de formas de violência política, por meio de iniciativas como:

  Tretaqui.org: realizará mapeamento da disseminação de conteúdos de ódio ou discriminatórios proferidos contra campanhas e fornecimento de canais de denúncia para as violações de direitos humanos praticadas durante o pleito eleitoral.

  Observatório de Candidaturas Femininas da OAB-SP: receberá denúncias de violações de direitos de candidatas mulheres no estado de São Paulo. O foco não é necessariamente sobre violência política online.

  Aliança Nacional LGBTI: está montando um grupo de advogados para receber e orientar denúncias de ataques LGBTfóbicos contra candidaturas LGBTs

Câmara dos Deputados: disponibilizará canal de denúncias de violência política no *Fale Conosco da Casa*.

SaferNet: em parceria com o MPF, a partir das denúncias que recebe, pretende oferecer elementos para a investigação de crimes eleitorais praticados a partir da web.

Referências

1. *http://www.tre-pi.jus.br/imprensa/noticias-tre-pi/2020/Julho/democracia-digital-eleicoes-2020-talk-show-virtual-reune-instituicoes-em-debate-sobre-desinformacao*

2. *http://www.tse.jus.br/imprensa/noticias-tse/2020/Maio/ultimo-video-da-serie-minuto-da-checagem-alerta-sobre-as-consequencias-da-divulgacao-de-desinformacao*

3. *http://www.tse.jus.br/imprensa/noticias-tse/2020/Julho/tse-faz-campanha-contra-a-desinformacao-201cse-for-fake-news-nao-transmita201d*

4. Incluído pela Lei nº13.834, de 2019, a medida será aplicada pela primeira vez nestas eleições.

5. Já tem sido aplicada em alguns casos relacionados à COVID- 19.