IV CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (IV CIDIA)

ALGORITMOS E DEMOCRACIA: DEFESA DE DIREITOS FACE À CULTURA DIGITAL

A396
Algoritmos e democracia: defesa de direitos face à cultura digital [Recurso eletrônico on-line] organização IV Congresso Internacional de Direito e Inteligência Artificial (IV CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: José Adércio Leite Sampaio, Meire Aparecida Furbino Marques e Lavínia Assis Bocchino – Belo Horizonte: Skema Business School, 2023.

Inclui bibliografia
ISBN: 978-65-5648-776-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os direitos dos novos negócios e a sustentabilidade.
1. Direito. 2. Inteligência artificial. 3. Tecnologia. I. IV Congresso Internacional de Direito e Inteligência Artificial (1:2023 : Belo Horizonte, MG).

CDU: 34

IV CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (IV CIDIA)

ALGORITMOS E DEMOCRACIA: DEFESA DE DIREITOS FACE À CULTURA DIGITAL

Apresentação

O IV Congresso Internacional de Direito e Inteligência Artificial - CIDIA da SKEMA Business School Brasil, realizado nos dias 01 e 02 de junho de 2023 em formato híbrido, consolida-se como o maior evento científico de Direito e Tecnologia do Brasil. Estabeleceram-se recordes impressionantes, com duzentas e sessenta pesquisas elaboradas por trezentos e trinta e sete pesquisadores. Dezenove Estados brasileiros, além do Distrito Federal, estiveram representados, incluindo Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Pará, Pernambuco, Paraná, Rio de Janeiro, Rio Grande do Norte, Rondônia, Roraima, Rio Grande do Sul, Santa Catarina, Sergipe, São Paulo e Tocantins.

A condução dos trinta e três grupos de trabalho do evento, que geraram uma coletânea de vinte e cinco livros apresentados à comunidade científica nacional e internacional, contou com a valiosa colaboração de sessenta e três professoras e professores universitários de todo o país. Esses livros são compostos pelos trabalhos que passaram pelo rigoroso processo de double blind peer review (avaliação cega por pares) dentro da plataforma CONPEDI. A coletânea contém o que há de mais recente e relevante em termos de discussão acadêmica sobre a relação entre inteligência artificial, tecnologia e temas como acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, sustentabilidade, democracia e responsabilidade civil, entre outros temas relevantes.

Um sucesso desse porte não seria possível sem o apoio institucional de entidades como o CONPEDI - Conselho Nacional de Pesquisa e Pós-graduação em Direito; o Programa RECAJ-UFMG - Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais; o Instituto Brasileiro de Estudos de Responsabilidade Civil - IBERC; a Comissão de Inteligência Artificial no Direito da Ordem dos Advogados do Brasil - Seção Minas Gerais; a Faculdade de Direito de Franca - Grupo de Pesquisa Políticas Públicas e Internet; a Universidade Federal Rural do Semi-Árido - UFERSA - Programa de Pós-graduação em Direito - Laboratório de Métodos Quantitativos em Direito; o Centro Universitário Santa Rita - UNIFASAR; e o Programa de Pós-Graduação em Prestação Jurisdicional e Direitos Humanos (PPGPJDH) - Universidade Federal do Tocantins (UFT) em parceria com a Escola Superior da Magistratura Tocantinense (ESMAT).

Painéis temáticos do congresso contaram com a presença de renomados especialistas do Direito nacional e internacional. A abertura foi realizada pelo Professor Dierle Nunes, que discorreu sobre o tema "Virada tecnológica no Direito: alguns impactos da inteligência artificial na compreensão e mudança no sistema jurídico". Os Professores Caio Lara e José Faleiros Júnior conduziram o debate. No encerramento do primeiro dia, o painel "Direito e tecnologias da sustentabilidade e da prevenção de desastres" teve como expositor o Deputado Federal Pedro Doshikazu Pianchão Aihara e como debatedora a Professora Maraluce Maria Custódio. Para encerrar o evento, o painel "Perspectivas jurídicas da Inteligência Artificial" contou com a participação dos Professores Mafalda Miranda Barbosa (Responsabilidade pela IA: modelos de solução) e José Luiz de Moura Faleiros Júnior ("Accountability" e sistemas de inteligência artificial).

Assim, a coletânea que agora é tornada pública possui um inegável valor científico. Seu objetivo é contribuir para a ciência jurídica e promover o aprofundamento da relação entre graduação e pós-graduação, seguindo as diretrizes oficiais da CAPES. Além disso, busca-se formar novos pesquisadores na área interdisciplinar entre o Direito e os diversos campos da tecnologia, especialmente o da ciência da informação, considerando a participação expressiva de estudantes de graduação nas atividades, com papel protagonista.

A SKEMA Business School é uma entidade francesa sem fins lucrativos, com uma estrutura multicampi em cinco países de diferentes continentes (França, EUA, China, Brasil e África do Sul) e três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua dedicação à pesquisa de excelência no campo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital requer uma abordagem transdisciplinar.

Expressamos nossos agradecimentos a todas as pesquisadoras e pesquisadores por sua inestimável contribuição e desejamos a todos uma leitura excelente e proveitosa!

Belo Horizonte-MG, 14 de julho de 2023.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Caio Augusto Souza Lara

Coordenador de Pesquisa – SKEMA Law School for Business

BLOCKCHAIN NO COMBATE À DESINFORMAÇÃO (FAKE NEWS) NA POLÍTICA BRASILEIRA

BLOCKCHAIN IN FIGHT AGAINST DISINFORMATION (FAKE NEWS) IN BRAZILIAN POLITICS

Meire Aparecida Furbino Marques [1]
Lavinia Assis Bocchino [2]

Resumo

A propagação de desinformação configura abuso da liberdade de expressão e pode macular o cenário eleitoral, comprometendo o exercício democrático. Neste estudo, propõe-se a utilização do blockchain, como meio de prova célere e segura no combate à desinformação e à investida de verdadeiras milícias digitais que pretendem manipular as eleições por meio de propagação em massa de informações falsas ou distorcidas. Aplicou-se, nesta pesquisa, o método normativo-dedutivo, fundado em revisão bibliográfica nacional e estrangeira, para demonstrar a necessidade de utilizar mecanismos que resguardem o processo eleitoral e a própria democracia.

Palavras-chave: Blockchain, Desinformação (fake news), Processo eleitoral. democracia

Abstract/Resumen/Résumé

The spread of disinformation constitutes an abuse of freedom of expression and can tarnish the electoral scenario, compromising the exercise of democracy. In this study, we propose the use of blockchain as a fast and secure means of proof to combat disinformation and the onslaught of real digital militias that intend to manipulate elections through the mass propagation of false or distorted information. In this research, the normative-deductive method was applied, based on national and foreign literature review, to demonstrate the need to use mechanisms that safeguard the electoral process and democracy itself.

Keywords/Palabras-claves/Mots-clés: Blockchain, Disinformation (fake news), Electoral process, Democracy

[1] Doutora e Mestre em Direito Público pela PUC-MG/BRASIL. Especialista em Direito Público, Tributário e Constitucional. Bacharel em Direito e Administração.

[2] Mestre em Constitucionalismo democrático pela PUC-MG/BRASIL, com bolsa da CAPES-PROEX. Pós-Graduada em Direito Digital (ITS/UERJ/CEPED). Bacharel em Direito.

Introdução

Na era digital, a democracia vem enfrentando grandes dificuldades, diante da ameaça ao exercício pleno da cidadania, principalmente, quanto as barreiras postas ao acesso à informação de qualidade e verídica, que viabiliza um debate público consciente. Para trabalhar o tema, a metodologia aplicada foi o método normativo-dedutivo, fundado em revisão bibliográfica nacional e estrangeira. O problema da desinformação massiva popularizou-se com o termo *fake news* (notícias falsas). Contudo, este não é um vocábulo adequado, pois nem todo conteúdo está em formato de notícia e nem sempre se trata de um conteúdo falso. Diante da inadequação do termo '*fake news'*, Claire Wardle (2019) sugere que esse conjunto de fenômenos da desinformação deva se chamar 'distúrbios da informação'.

Propagar intencionalmente desinformação para manipular o debate democrático constitui abuso do direito à liberdade de expressão. Remover esse conteúdo ilícito das redes sociais é medida que se impõe. Contudo, na prática, há uma linha tênue cercada de subjetividade que dificulta definir quais são os limites da livre manifestação de pensamento e o que configura censura. E, mesmo assim, a remoção, ainda que utilizada nos casos mais evidentes de violação a direitos, não garante solucionar o problema, em seu nascedouro.

O que se enfrenta, na atualidade virtual, são volumes de desinformação incontroláveis propagados a cada segundo, que não se resume apenas a conduta de um indivíduo, mas de verdadeiras milícias digitais. A partir da análise do Inquérito das Fake News e da CPI da Pandemia COVID-19 é possível compreender a estrutura dessas organizações e os motivos que dificultam sua identificação e responsabilização (BRASIL, 2021).

É certo que existem variadas alternativas para tentar combater a desinformação, como a alfabetização midiática, o emprego de inteligência artificial (IA), o *machine learning*, as agências de checagem de fatos, as parcerias da justiça eleitoral com as redes sociais, entre outras. No presente o estudo, analisa-se o emprego do *blockchain*. A novidade desse sistema, que recentemente vem sendo aceita pelos tribunais brasileiros, é sua celeridade e custo/benefício para autenticar determinada informação, assegurando-lhe fidúcia e rastreabilidade.

Essa ferramenta possibilita, por exemplo, que candidatos políticos se previnam contra eventuais maculações que venham a ser feitas em seus documentos e publicações oficiais, pois é uma maneira mais célere de autenticar arquivos. Além disso, uma vez feito o registro no sistema, é possível comparar com imagens, texto, vídeos veiculados na internet para verificar se se trata de cópia falsificada para propagar desinformação sobre o candidato.

1.*Blockchain*: conceito e aplicação

Ferramentas tecnológicas (IA, algoritmos e *machine learning*) estão em voga quando as questões que se pretende resolver abarcam um grande volume de dados e se propagam rapidamente. O *blockchain* também vem se apresentando como uma promissora alternativa no combate à desinformação especialmente por sua segurança, pois, a rigor, é um meio mais difícil de ser hackeado.

Mas o que é *Blockchain*? Trata-se de uma ferramenta que funciona como um livro razão ao registrar transações, no qual as cópias de um conteúdo são distribuídas entre todos os computadores da rede e são atualizadas a cada nova transação. Essa tarefa é feita pelo próprio sistema, não necessita de seres humanos e empresas, ou seja, não é mantido por um grupo centralizado, mas por uma rede de computadores (EXPLICANDO…, 2018). A partir disso, tem-se a imparcialidade e consequente confiança no que se intenta guardar, buscar ou compartilhar por esse meio.

As redes apresentam uma 'arquitetura', cujos modelos são: (1) centralizado, que tem uma alta vulnerabilidade, pois todas as máquinas estão ligadas a uma única rede, isso significa que se a rede central cai, todas as outras deixam de funcionar; (2) descentralizado, em que há mais de uma rede central, então ainda que uma caia, haverá outros servidores funcionando; e, por fim, (3) o sistema de rede distribuída ou *peer-to-peer*, no qual todos os computadores estão conectados na rede *blockchain*, ou seja, todos têm acesso à mesma informação e são independentes (MENEZES, 2022).

O protocolo de confiança no terceiro modelo de rede funciona da seguinte forma: qualquer tipo de transação deve ser validada por todos os computadores, como uma espécie de consenso, bem como todos os registros são feitos informando a data e a hora; ordinariamente são imutáveis, de modo que não há a possibilidade de se desfazer uma transação e os arquivos são criptografados por meio de um sistema alfanumérico (MENEZES, 2022)

Quanto à criptografia, existem dois sistemas: (1) simétrico, que possui apenas uma chave pública, esta serve para encriptar e desencriptar uma informação, por exemplo, para uma pessoa ler a mensagem que lhe foi enviada ela precisa ter a mesma chave de quem a enviou, e o problema nesse processo é que alguém pode fazer a interceptação dessa troca de informações; por outro lado, (2) na criptografia assimétrica, utilizada no *blockchain*, além da chave pública, utilizada para encriptar uma informação, existe também a chave privada para desencriptar conteúdos, tratando-se pois de uma maneira mais segura no compartilhamento de dados, já que

não é necessário compartilhar a chave que vai desencriptar a mensagem, sendo ela única para cada usuário e não compartilhável como na pública (MENEZES, 2022)

Importante ressaltar que há *blockchain* de rede pública e privada. A privada é fechada apenas para o grupo de pessoas que a utiliza e geralmente são editáveis, ao contrário da rede pública do *blockchain*. No Brasil, atualmente, apenas empresas privadas aplicam esse sistema para as eleições. É um serviço que previne a desinformação, garantindo autenticidade e meios de rastrear os dados, diferente das agências de checagem de fatos que, apesar da tarefa essencial desempenhada, cuidam somente de comparar um conteúdo falso publicado com o fato real. (MENEZES, 2022)

O *blockchain* aplicado às eleições não impede a fabricação de *fake news* mas dificulta esse tipo de conduta, além de garantir maior fidúcia à fonte de uma informação e impedir a veiculação de cópias não autorizadas do documento que foi autenticado. Segundo Ronaldo B. Do Val, Thamirys D. Viana e Luis B. Gouveia (2021), após os documentos digitais serem validados como verdadeiros na rede *blockchain*, o sistema consegue identificar as postagens falsas feitas sobre o conteúdo original. Ademais, asseveram os autores que "uma vez que a informação é registrada na *blockchain*, os leitores podem ter certeza de sua autenticidade" (VAL; VIANA; GOUVEIA, 2021, p. 273), o que passa a ser bastante eficaz, pois o tempo não é suficiente para verificar o volume de conteúdo compartilhado na internet.

Isso significa que uma agência de notícia, devido a rastreabilidade, ainda que em diferentes formatos como texto, imagens e vídeos, e imutabilidade de um arquivo registrado no *blockchain*, pode garantir a segurança da fonte de uma informação, nome da empresa e do jornalista da matéria, além do próprio conteúdo veiculado. Esse procedimento ocorre por meio de um Contrato Inteligente (Smart Contract) entre o consumidor e o fornecedor desse serviço, o que promove maior transparência e descentralização na abordagem.

Acrescente-se que os fornecedores desses serviços utilizam a técnica *hash*, que a partir de algoritmos realiza uma análise comparativa de arquivos para verificar a integridade do conteúdo (VAL; VIANA; GOUVEIA, 2021). Esse processo pode ser aplicado por candidatos em campanhas eleitorais, por exemplo, para autenticar seu plano de governo, impedindo alterações em seu conteúdo. Especificamente para o período das eleições, no qual os eventuais problemas precisam ser resolvidos rapidamente devido aos prazos curtos da justiça eleitora, a tecnologia *blockchain* apresenta dois pontos positivos: (1) celeridade e praticidade: a autenticação de um conteúdo por *blockchain* é disponibilizado no momento da transação e pode ser feito a qualquer momento, ao contrário de um cartório de registro em que a rigor requer a presença física do solicitante ou agendamento; (2) custo/benefício: comparado ao valor da ata

notarial em cartórios de registro, a pessoa que precisa autenticar um documento pode utilizar da rede pública de *blockchain* que é gratuita, ou até mesmo a privada, que oferece baixo custo.

Diante das diversas manobras de se macular uma informação, editando-a para apresentar um conteúdo falso, o Superior Tribunal de Justiça, publicou decisão em 30/08/2021, referente ao Recurso Especial nº 1.903.273, deliberando que *prints* de tela de conversas de *WhatsApp* não podem ser utilizadas como meio de prova válido (BRASIL, 2021). Nesse contexto, em prol da vitória na disputa judicial é importante que as partes procedam de forma preventiva e apresentem documentos autenticados para comprovação de sua veracidade, principalmente quando se trata de conteúdo ofensivo postado na internet, que pode ser rapidamente excluído sem deixar rastros, daí a necessidade de uma certificação para assegurar-lhe sua existência.

Cabe ressaltar, que em tais casos, a ata notarial dos cartórios de registros possui fé pública, portanto são aceitas pelo judiciário. Contudo, são mais caras e lentas comparadas ao serviço de *blockchain*, que recentemente vem sendo aceito pelos tribunais brasileiros. Estela Aranha, reforça o reconhecimento do *blockchain* como interface sólida para a apresentação de provas em tribunais (SANTOS, 2020). Apesar da linha tênue a respeito da matéria, importa ressaltar que o direito à liberdade de expressão é fundamental para o exercício democrático, contudo não é absoluto. A própria Constituição brasileira impõe limitações às condutas que ferem a honra, a intimidade, a vida privada e a imagem da pessoa (CF/88). Nesse sentido, o Superior Tribunal Federal ao reconheceu que a liberdade de expressão não abarca opiniões criminosas, discurso de ódio ou atentados contra o Estado Democrático de Direito (AP 1044/DF). A pretensão de macular o voto do eleitor por meio da disseminação de desinformação viola os princípios e as garantias da Constituição Federal e pode desvirtuar o processo democrático e a interferir na soberania popular, pois o poder vem do povo com o voto livre.

E não apenas no Brasil. Tem-se, por exemplo, a aplicação do *blockchain* no Referendo da Macedônia, cujo escopo foi garantir maior lisura ao debate público sobre temas de grande relevância para a população: a adesão do país à Organização do Tratado do Atlântico Norte e à União Europeia. A iniciativa Trusted Public Report em parceria com a Design 4 Democracy Coalition, Blockchain Trust Accelerator (BTA) e Emercoin cuidaram para que os cidadãos tivessem acesso aos documentos públicos livres de falsificação, pois eram registrados em *blockchain*. A técnica funcionava da seguinte maneira: primeiro, criou-se o evento do referendo na plataforma com uma lista de organizações examinadas; o segundo passo foi a anexação de um relatório ao sistema *blockchain*, pela organização avaliada; por fim, estando o arquivo

devidamente registrado e autenticado, a última etapa foi disponibilizar o documento verificado para o público por meio do site (TRUSTED PUBLIC REPORT, 2019).

No histórico eleitoral brasileiro recente, já se percebe a utilização de tecnologias baseadas em *blockchain* como serviços voltados à redução de impactos da divulgação de desinformação sobre a campanha de candidatos. Nas eleições municipais de 2020 a startup brasileira OriginalMy comercializou uma ferramenta voltada à validação da veracidade de conteúdos difamatórios sobre candidatos divulgados na internet.

A iniciativa de utilização de *blockchain* em períodos eleitorais, não é inédita no cenário global. A imutabilidade das informações publicadas por meio de *blockchain* permite a garantia de autenticidade de conteúdos publicados na internet. Os serviços ofertados pela startup brasileira, chamados Prova de Autenticidade de Conteúdo Eleitoral (PAC Eleitoral) e Prova de Autenticidade de Conteúdo Digital (PAC Digital) funcionam nesse sentido. Candidatos que contratarem os serviços conseguem comprovar, com o suporte da OriginalMy, se determinados materiais de campanha publicados online de fato foram gerados pelos candidatos, evitando possíveis alterações, modificações ou cópias dos seus conteúdos. (SANTOS, 2020)

Na prática, a utilização corriqueira de tecnologias e serviços voltados à verificação da veracidade das informações dispostas online auxilia na detecção da natureza da informação que está sendo disponibilizada aos clientes, a partir do momento que a tecnologia também alcance esses usuários. Um dos serviços ofertados pela startup OriginalMy1 é o Prova de Autenticidade de Conteúdo Web (PACWeb), que dinamiza a coleta de informações orientadas à validação da veracidade do conteúdo, emitindo um relatório a partir do acionamento do usuário que servirá como prova, porventura em tribunais de justiça, da publicação de conteúdos alterados ou difamatórios.

Cabe ressaltar também que, para além da utilização dos serviços da OriginalMy por parte de clientes, usualmente políticos em época de eleição, também há a disponibilização no site da empresa de um campo para a submissão, por parte do público em geral, de denúncias sobre casos de inautenticidade de conteúdo ou desobediência das regras eleitorais. É sabido, no entanto, que a possibilidade de veiculação de *fake news* na internet ainda permanece no cenário eleitoral brasileiro, mesmo com a existência de ferramentas de verificação de autenticidade de publicações via *blockchain*. O referido serviço não é imune a críticas. Percebe-se, por exemplo, a inexistência de fases concernentes à verificação da veracidade do conteúdo publicado, ou seja,

[1] Para melhor compreender o procedimento da PACWeb da OriginalMy acesse o vídeo ilustrativo disponível em: https://originalmy.com/pacweb . Acesso em: 15 jul. 2022.

não há um controle de que as publicações que estão sendo autenticadas via *blockchain* não corroboram na veiculação de desinformação. Acerca das problemáticas da desinformação, Priscilla Menezes ressalta que "[...] é importante descobrir o caminho do dinheiro, quem está veiculando, financiando e lucrando com isso. A ferramenta (PAC Eleitoral) é interessante, mas não é suficiente para dar conta desse cenário bizarro que a gente tem hoje" (SANTOS, 2020, s.p).

Ademais, o *blockchain* aplicado no cenário eleitoral, embora auxilie na proteção dos políticos quando são alvos de ataques de desinformação, implica que os candidatos tenham conhecimento sobre esse meio, seja no âmbito público ou privado. Ainda assim, não se procede automaticamente à verificação das cópias falsificadas na internet: é necessário primeiro localizar as publicações indevidas para, após, utilizar-se da referida tecnologia para comparar o conteúdo suspeito com aquele registrado na rede *blockchain*.

Essa ferramenta desestimula a propagação de desinformação, uma vez que garante de forma célere a autenticação da origem de determinado conteúdo e a prova quanto a existência de eventuais alterações do documento original, dificultando as atividades ilícitas de uma milícia digital. Cabe pontuar, que o *blockchain* é mais uma dentre outros meios nessa luta contra as *fake news*, disseminadas nas redes sociais. Nesse sentido, destaca-se a importância do investimento em alfabetização midiática da população, o dever das instâncias do judiciário de melhor fiscalizarem e aprimorarem a persecução sancionatória, como por exemplo pela técnica *follow the money*, que seria investir nas investigações que rastreiam o dinheiro que financia a indústria da desinformação, bem como, o fortalecimento normativo para regulação das novas tecnologias, como a recente aprovação do Projeto de Lei 2.630/2020.

Conclusão

A livre discussão, a ampla participação política e o princípio democrático estão interligados com a liberdade de expressão, tendo por objetivo não somente a proteção de pensamentos e ideias, mas também opiniões, crenças, no sentido de garantir a real participação dos cidadãos na vida coletiva. Qualquer abuso desse direito com o fim de macular o debate público deve ser veemente tolhido. Assim, medidas como *blockchain* auxiliam no combate à desinformação, pois possibilitam uma maneira mais célere e segura de autenticação de conteúdo, bem como, de verificar quais as eventuais cópias falsificadas compartilhadas na internet. Nesse cenário, principalmente diante das *deep fakes*, a aplicação dessa ferramenta é interessante, pois após a autenticação do documento original, seja em formato de vídeo, texto e

imagem, pode ser rastreado e comparado com suas cópias na internet, podendo detectar eventuais edições indevidas.

Referências

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 27 jun. 2021.

EXPLICANDO: Criptomoedas. Produção: Frank Matt. Local de Publicação: Netflix, 06 jun. 2018.

MENEZES, Priscilla. **Direito e Blockchain.** Na Pós-Graduação em Direito Digital da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ) em parceria com o Instituto de Tecnologia e Sociedade (ITS). Rio de Janeiro: UERJ e ITS, 2022.

ORIGINALMY. **OriginalMy**: PACWeb. 2022. Disponível em: https://originalmy.com/pacweb. Acesso em: 15 jul. 2022.

SANTOS, Cleberson. Como uma startup tem usado blockchain para lutar contra fake news. **Tilt uol**, p. s.p, 21 out. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/10/22/eleicoes-como-uma-startup-tem-usado-blockchain-para-lutar-contra-fake-news.htm Acesso em: 06 set. 2022

BRASIL. Senado Federal: **Comissão Parlamentar de Investigação da Pandemia COVID-19**: Relatório Final da CPI da Covid-19. Autoria: Senador Renan Calheiros, 26 out. 2021. Disponível em: https://legis.senado.leg.br/comissoes/mnas?codcol=2441&tp=4 Acesso em: 06 set. 2021.

SUPERIOR TRIBUNAL DE JUSTIÇA. STJ. Divulgação de mensagens do WhatsApp sem autorização pode gerar obrigação de indenizar. **STJ Notícias** , p. s.p, 2 set. 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/02092021-Divulgacao-de-mensagens-do-WhatsApp-sem-autorizacao-pode-gerar-obrigacao-de-indenizar-.aspx. Acesso em: 10 jul. 2022.

TRUSTED PUBLIC REPORT. **Defending Information Integrity**: Blockchain-Powered Notary. 2019. Disponível em: https://democracynotary.org/en.html. Acesso em: 15 jul. 2022.

VAL, Ronaldo Borges do; VIANA, Thamirys Dias; GOUVEIA, Luis Borges. **O uso de Blockchain na identificação de Fake News:** ferramentas de apoio tecnológico para o combate à desinformação. Brazilian Journals of Business (BJB), Curitiba, ano 2021, v. 3, n. 3, p. 2726-274, 16 ago. 2021. DOI https://doi.org/10.34140/bjbv3n3-050. Disponível em: https://brazilianjournals.com/ojs/index.php/BJB/article/view/34564. Acesso em: 6 jul. 2022.

WARDLE, Claire. **FIRST DRAFT'S Essential Guide to Understanding Information Disorder.** First Draft, October 2019.