PERÍCIA DIGITAL E TEORIA DA CORRELAÇÃO ENTRE ACUSAÇÃO E SENTENÇA: DIFERENCIANDO *FAKE NEWS* E CALÚNIA NAS REDES SOCIAIS

Marcos De Lucca Fonseca
Sebastião Augusto de Camargo Pujol

RESUMO: O presente artigo tem por objetivo discorrer sobre como a perícia digital, com base na eficaz aplicação da Teoria da Correlação entre Acusação e Sentença, é fundamental para a diferenciação entre a imputação do delito do artigo 326-A do Código Eleitoral - conhecido como crime de *fake news* com finalidade eleitoral - e o crime de calúnia (art. 138 do Código Penal) cometidos nas redes sociais. Serão indicados os conceitos e as etapas a serem seguidas pela perícia digital, e, em especial, a cadeia de custódia para garantir a integridade da prova digital, para evidenciar e diferenciar as condutas dos tipos penais analisados.

PALAVRAS-CHAVE: Direito Penal, *Fake News,* Eleitoral, Teoria da Correlação Entre Acusação e Sentença; Prova Digital, Perícia Digital, Cadeia de Custódia da Prova Digital. Computação Forense. Internet. Redes Sociais. Crimes Informáticos.

INTRODUÇÃO: a era da pós-verdade

Tecendo olhar para a nossa sociedade atual, com o acelerado uso e desenvolvimento de novas tecnologias de comunicação e informação, o indivíduo pode se deparar com um contexto jamais visto ou experimentado. Essa percepção pode mudar a forma como ele se relaciona consigo, com os seus semelhantes e com o meio social – chegando, até mesmo, a ter impacto no sistema econômico, político-social e cultural, como descreve Eric Schmidt e Jared Cohen "o modo como interagimos e vemos a nós mesmos continuará sendo influenciado e conduzido pelo mundo on-line ao nosso redor".[8]

A tecnologia da informação alterou profundamente vários aspectos da interrelação social, transformando mercados, processos produtivos, relacionamentos sociais, instituições e até mesmo, as relações de trabalho. Como não podia ser diferente, com a "virtualização

[8] SCHMIDT, Eric. COHEN, Jared, "A nova era digital". editora intrínseca. 2013. p. 13

da vida", novas condutas delitivas surgiram deste recente comportamento virtual.

Até a invenção da imprensa móvel, por Johannes Gutenberg, em meados de 1455, a divulgação da informação estava restrita e concentrada nas mãos de uma elite política e religiosa.[9]

Como tal divulgação estava restrita e dependia dos trabalhos dos copistas, era relativamente mais "fácil" controlar o dissenso e a disseminação de uma informação que não fosse de interesse da elite. Com a invenção de Gutenberg, além de a informação ser divulgada a menor custo, sua velocidade aumentou consideravelmente. A disseminação de informação através da criação da prensa móvel trouxe profundas alterações no *status quo*, tendo consequências na ordem social, econômica, política e até religiosa, pois foram divulgadas ideias e informações que contribuíram para essas mudanças – em especial as teses de Martinho Lutero que, por meio da prensa móvel, foram impressas na ordem de mais de 250 mil vezes em pouco intervalo de tempo[10], e contribuíram para o enfraquecimento do sistema feudal.

Para muitos estudiosos da imprensa, o surgimento de sua expressão digital e das redes sociais, no final do século 20 e início do século 21, poderia ser equiparado ao surgimento da prensa tipográfica. Tanto no contexto de Lutero quanto no advento das redes televisivas, o custo da comunicação era muito grande e ficava concentrado nas mãos de uma elite. A grande novidade, com o advento das tecnologias digitais e, em especial das redes sociais, foi justamente a considerável diminuição do custo de divulgação da informação. Como mencionado por Mounk (2018), "o custo da informação um-para-muitos fora democratizado, mais de quinhentos anos depois"[11] do surgimento da imprensa.

No início da utilização da tecnologia da informação, em especial da internet, a divulgação das informações foi concentrada em *websites*. Mas é evidente que uma página na internet de um grande grupo da indústria de comunicação ainda teria, além de mais credibilidade, maior alcance de divulgação. Mesmo que essa nova configuração fosse uma oportunidade para que indivíduos marginalizados pelos conglomerados de comunicação pudessem exercer certa

[9] Disponível em: https://super.abril.com.br/mundo-estranho/como-funcionava-a-prensa-de-gutenberg/ Acesso em: 04 mai.2020.

[10] MOUNK, Yascha. *O povo contra a democracia.* São Paulo: Companhia das Letras, 2018, p.170.

[11] MOUNK, Yascha. *O povo contra a democracia.* São Paulo: Companhia das Letras, 2018, p.172.

influência na formação de opinião, o *gap* do raio de influência que ele exercia frente aos demais grupos de mídia ainda era bem considerável.

Entretanto, com o surgimento das redes sociais, o "raio de influência" do indivíduo foi consideravelmente ampliado. Se uma pessoa produzisse um conteúdo que pudesse ser interessante e tivesse a divulgação fora de seus contatos, poderia ampliar notavelmente a distribuição de sua mensagem. Assim, surgiu a comunicação "muitos-para-muitos"[12]. As redes sociais, em especial com os eventos realizados pela chamada "Primavera Árabe", incentivaram protestos realizados pela internet. Alguns, inclusive, chegaram a organizar, pelas redes sociais, protestos que ocorreram nas ruas.

1. Redes sociais e política

Não há como negar que o exponencial aumento da utilização das redes sociais trouxe consequências e aumentou, de certa forma, a participação da população geral na discussão dos temas políticos nacionais e internacionais. Alguns analistas, a propósito, afirmaram que a internet poderia se tornar a nova "Ágora", concentrando as discussões políticas da sociedade contemporânea.

Mas como todo instrumento de comunicação, que pode ser utilizado tanto para auxiliar no desenvolvimento de boas ideias e debates quanto para não contribuir positivamente e divulgar informações de origem e conteúdo duvidosos, assim também ocorreu com as redes sociais. Além disso, incitou-se uma análise de como os regimes políticos e os grupos extremistas poderiam utilizar o alto poder de divulgação que as redes sociais possuem.

Para Mounk (2018), a campanha eleitoral de Donald Trump foi um divisor de águas na utilização das redes sociais e sobre como os chamados veículos de comunicações tradicionais deveriam se inter-relacionar com essa nova realidade. Se Trump não tinha "espaço" nos veículos de comunicação tradicionais (como emissoras de rádio, TV, jornais impressos ou até mesmo *websites*), ele utilizava as redes sociais para divulgar suas mensagens – mesmo as mais polêmicas. Com isso, conseguiu manter o diálogo com seus eleitores e, além disso, pautou o jornalismo tradicional, uma vez que os jornais acabavam por comentar as suas declarações veiculadas nessas redes.

[12] Idem, p.173.

As chamadas "câmaras de eco"[13] foram utilizadas pelos políticos de forma indireta, pois a divulgação de mensagens ideológicas e massivas polarizaram cada vez mais o debate político. Trazendo uma sensação de que o indivíduo está interagindo com o mundo exterior, os algoritmos das redes sociais podem definir, e até mesmo limitar, as notícias e informações que as pessoas acessam. Assim, a interação com pessoas e páginas de aplicativo de uma rede social, com conteúdo em que o indivíduo se identifica, chega até mesmo a limitar o acesso na internet – como uma espécie de mecanismo de retroalimentação das informações e um espaço em que o indivíduo escuta e tem acesso às informações somente de acordo com suas convicções pessoais.

Se em um primeiro momento as redes sociais eram vistas como uma ferramenta que pudesse contribuir e auxiliar o desenvolvimento da democracia, agora pode ser vista com ressalvas, sendo considerada como uma das principais ameaças contemporâneas à democracia e aos valores republicanos. Não se trata de promover uma discussão maniqueísta sobre a utilização das mídias sociais no debate político. Se bem utilizadas, tais mídias podem, com toda certeza, contribuir para o aprimoramento do debate político ou até mesmo ser utilizadas como meio de resistência em países com regimes políticos não democráticos.

Outro ponto que deve ser considerado, é a rapidez e facilidade ao acesso dos indivíduos aos *smartphones*, se comparados com o demorado acesso aos livros que foram resultado do surgimento da prensa móvel. Pouco mais de uma década após o surgimento das redes sociais, mais de 2 bilhões de pessoas as utilizam.

1.1. Declaração da OEA sobre a liberdade de expressão e eleições na era digital

No dia 30 de abril de 2020, a Organização dos Estados Americanos (OEA) publicou como parte das comemorações do Dia Mundial da Liberdade de Imprensa, a "Declaração Conjunta sobre Liberdade de Expressão e Eleições na Era Digital"[14]. Nela, consta

[13] Os algoritmos implementados pelos sites de mídias sociais para fornecer conteúdo personalizado claramente desempenha um papel importante em garantir que os usuários encontrem apenas informações que correspondam às suas crenças. Disponível em: https://exame.abril.com.br/tecnologia/a-surpreendente-velocidade-que-nos-tornou-polarizados-on-line/ Acesso em: 04 mai. 2020.

[14] Disponível em: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1174&lID=2 Acesso em: 10 mai. 2020.

uma série de recomendações aos seus Estados-Membros.

Com uma gama de princípios gerais, a Declaração recomenda aos Estados o estabelecimento de um marco regulatório que promova a liberdade, a independência e a diversidade dos meios de comunicação – tanto na mídia tradicional quanto nos meios digitais. Essas recomendações principiológicas podem estar relacionadas à questões de liberdade de expressão, mas o que há de mais novo na Declaração de 30 de abril de 2020 é justamente a preocupação que a OEA tem em relação à importância dos Estados garantirem aos seus eleitores acesso à informação de forma ampla, precisa e confiável sobre os partidos políticos, os candidatos e à totalidade do processo eleitoral.

Sem deixar de mencionar que os Estados devem garantir aos indivíduos o efetivo acesso à rede mundial de computadores, através de políticas públicas que de fato promovam tal acesso, a OEA destacou que os Estados não devem censurar os meios de comunicação, incluindo o bloqueio a *websites* ou interrupções da prestação do serviço de acesso à internet. Parte-se do pressuposto de que os políticos, por serem figuras públicas, devem tolerar a exposição de suas imagens de forma mais razoável do que aquela tolerada por um cidadão comum, que tem um nível de exposição social bem menor.

Ainda de acordo com as recomendações da OEA, os Estados não devem criar leis genéricas ou ambíguas sobre a temática da "desinformação". Especialmente no período de realização de eleições, os meios de comunicação devem respeitar normas de imparcialidade e equilíbrio, oferecendo a todos os candidatos igualdade de condições para se comunicarem diretamente com o seu público. Outro ponto de preocupação que a OEA externa é sobre a utilização dos dados pessoais dos eleitores para o marketing a eles direcionado. Isso deve ocorrer tão somente se os titulares dos dados pessoais assim o permitirem, dando o seu consentimento e, desde que, seja utilizado para uma finalidade específica.

Em relação aos atores não estatais, em especial os atores digitais, a OEA sugere que as plataformas digitais adotem medidas que possibilitem aos usuários o acesso a diversas perspectivas e ideias políticas. Uma das preocupações dessa Organização Internacional é a utilização de algoritmos de classificação, amplamente utilizados pelas aplicações na internet. Esses serviços não devem, de forma intencional, obstaculizar a

disponibilidade de acesso a diversos pontos de vista.

Tratando especificamente das *fake news* com finalidade eleitoral, a Declaração da OEA também recomenda que os meios digitais promovam esforços para abordar o tema da "desinformação", da informação errônea ou manipulada de forma intencional. Inclusive propõe a promoção de instâncias de verificação independentes ou a implantação de outras medidas para tratar desses temas.

1.2. *Fake news* com finalidade eleitoral: a realidade no Brasil

Dando sequência ao desenvolvimento da problemática da utilização de *fake news* com finalidade eleitoral no Brasil, o centro independente de pesquisa interdisciplinar, Internetlab, publicou o seu relatório "Internet e eleições no Brasil: diagnósticos e recomendações"[15]. Esse relatório foi resultado de uma série de pesquisas que o Interlab realizou para estudar a desinformação e a sua utilização em campanhas políticas no Brasil, em especial nas eleições de 2018. Os principais pontos abordados pelo relatório foram a análise de questões como o crescimento da utilização da internet e a necessidade de utilização da rede nas campanhas eleitorais.

Não foi alterada somente a forma com que a informação é produzida e divulgada na era das redes sociais. Alterou-se também a forma como o indivíduo se relaciona com ela. E, quando se adiciona o ambiente de polarização política característico em um cenário de campanha eleitoral acirrada, a probabilidade de ocorrência de desinformação ganha uma escala sem precedentes em nossa recente história democrática.

Um dos principais aspectos e, que também é mencionado pelo relatório do Internetlab, é que as campanhas digitais não estão mais centralizadas nos partidos políticos, através da contratação de profissionais de marketing ou de comunicações. Mesmo que possa ocorrer ainda a contratação de empresas ou de aplicações, a chamada "militância digital" exerce protagonismo fundamental numa campanha eleitoral digital.

Ocorre que este novo "modelo" de campanha digital implicou uma crise do modelo regulatório eleitoral que, até

[15] BRITO CRUZ, Francisco (coord.); MASSARO, Heloisa; OLIVA, Thiago; BORGES, Ester. *Internet e eleições no Brasil: diagnósticos e recomendações.* São Paulo: InternetLab, 2019. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2019/09/policy-infopol-26919_4.pdf Acesso em 25 mai. 2020.

então, vigorava no Brasil. A campanha política estava direcionada às ruas e à televisão. E, nesses "ambientes", era facilitado o conhecimento de condutas ilícitas nas campanhas eleitorais. Outro ponto essencial e que não era utilizado nas campanhas eleitoras anteriores às digitais, é que aquelas não utilizavam (ao menos de forma direta) a coleta de dados pessoais dos eleitores. Já as campanhas digitais, além de coletarem os dados pessoais dos eleitores através de aplicações e de *cookies*[16], utilizam-se dessas ferramentas para microdirecionar a audiência e os materiais de campanha, bem como as desinformações – ou simplesmente as chamadas *fake news*.

A essência do chamado marketing de guerrilha[17], que buscava atingir objetivos convencionais por meio de métodos não convencionais, vai ganhando também a internet e as campanhas eleitorais digitais. Através da contratação dos chamados "impulsionadores de conteúdo", os *bots*[18] podem ampliar a visibilidade ou a "audiência virtual" e/ou apoiadores de candidatos. Assim, pode-se criar uma falsa impressão de que determinado assunto está sendo mais debatido, ou até mesmo que determinado candidato tem mais apoiadores do que de fato possui. O grande desafio, como consta no relatório do Internetlab, é como fiscalizar essas condutas.

Diante disso, a presente pesquisa reflete sobre como a perícia digital, com base na eficaz aplicação da Teoria da Correlação entre Acusação e Sentença, é fundamental para a diferenciação entre a imputação do delito do artigo 326-A do Código Eleitoral - conhecido como crime de *fake news* com finalidade eleitoral - e os Crimes contra a Honra do Código Penal cometidos no meio digital – mais especificamente a internet. Serão indicados os conceitos e as etapas a serem seguidas pela perícia digital e, em especial, a cadeia de custódia para garantir a integridade da prova digital, para evidenciar como os *bots* podem ser utilizados para alavancar postagens deste tipo de conteúdo, em redes sociais.

---

[16] Os *cookies* são arquivos de internet que armazenam temporariamente o que o internauta está visitando na rede. Disponível em:https://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-sao-cookies-e-como-eles-podem-me-prejudicar.html#rmcl Acesso em: 25 mai. 2020.

[17] O publicitário americano Jay Conrad Levinson foi quem desenvolveu esse termo, no final dos anos 1970. Utilizou a expressão para descrever ações de comunicação que fugissem do trivial, do comum. Disponível em: https://endeavor.org.br/marketing/marketing-de-guerrilha/?gclid=EAIaIQobChMI2O3R4tfQ6QIVIfC1Ch2qFA0pEAAYASAAEgJ1wPD_BwE Acesso em: 25 mai. 2020.

[18] *Bots* são como programas de computador criados para rodar pela internet realizando tarefas repetitivas e automatizadas. Disponível em: https://www.techtudo.com.br/noticias/2018/07/o-que-e-bot-conheca-os-robos-que-estao-dominando-a-internet.ghtml Acesso em: 25 mai. 2020.

1.3. A criação do tipo penal "*fake news* com finalidade eleitoral"

A Lei n. 13.834, aprovada em 04 de junho de 2019 – mas somente promulgada em 11 de novembro de 2019 após o Congresso Nacional derrubar os vetos do Presidente da República[19], tipificou o crime de denunciação caluniosa com finalidade eleitoral, alterando o Código Eleitoral ao incluir o art. 326-A[20] , cujo objetivo foi incriminar as chamadas "*fake news* com finalidade eleitoral". De acordo com o Relatório Final de Observação das Eleições Gerais do Brasil em 2018, da Organização dos Estados Americanos (OEA)[21], vários segmentos políticos que disputaram o pleito no ano de 2018 utilizaram sistemas e aplicações da internet para o envio de mensagens privadas e a divulgação em massa de desinformação.

Como destacado pelo próprio relatório da OEA, esse fenômeno não foi exclusivo das eleições do Brasil em 2018, mas também em outros países[22]. O relatório menciona que o Tribunal Superior Eleitoral (TSE) criou em dezembro de 2017 um Conselho Consultivo sobre internet e eleições, principalmente atentando para a alta disseminação das chamadas *fake news*[23] nas eleições gerais do Brasil que ocorreriam em 2018. O Conselho também destacou a possibilidade de utilização dos chamados *bots*[24]para divulgação em massa de informações falsas. Para se ter

19 Disponível em: https://veja.abril.com.br/politica/lei-contra-fake-news-eleitoral-e-promulgada-apos-congresso-derrubar-veto/ Acesso em: 20 abr. 2020.

20 Art. 326-A do Código Eleitoral: Dar causa à instauração de investigação policial, de processo judicial, de investigação administrativa, de inquérito civil ou ação de improbidade administrativa, atribuindo a alguém a prática de crime ou ato infracional de que o sabe inocente, com finalidade eleitoral:
Pena - reclusão, de 2 (dois) a 8 (oito) anos, e multa.
§ 1º A pena é aumentada de sexta parte, se o agente se serve do anonimato ou de nome suposto.
§ 2º A pena é diminuída de metade, se a imputação é de prática de contravenção.
§ 3º Incorrerá nas mesmas penas deste artigo quem, comprovadamente ciente da inocência do denunciado e com finalidade eleitoral, divulga ou propala, por qualquer meio ou forma, o ato ou fato que lhe foi falsamente atribuído.

21 Disponível em: http://www.oas.org/documents/por/press/MOE-Brasil-2018-Relatorio-Final-POR.pdf. Acesso em: 28 abr. 2020.

22 Disponível em: http://www.oas.org/documents/por/press/MOE-Brasil-2018-Relatorio-Final-POR.pdf p.13. Acesso em: 28 abr. 2020.

23 O conceito *fake news* é usado para se referir a notícias falsas ou imprecisas que são publicadas, majoritariamente, na internet. Essa expressão, que significa literalmente "notícias falsas" (em tradução livre), já existe há bastante tempo. Entretanto, ganhou popularidade após ser usada repetidamente pelo então candidato Donald Trump, durante as últimas eleições presidenciais dos Estados Unidos, em 2016, e foi, inclusive, considerada a palavra do ano em 2017 pelo dicionário Collins.
Disponível em: https://www.techtudo.com.br/noticias/2018/01/o-que-sao-fake-news-veja-dicas-para-identificar-boatos-na-internet.ghtml Acesso em: 28 abr. 2020.

24 Os *bots* são aplicações autônomas que rodam na internet enquanto desempenham algum tipo de tarefa pré-determinada. Eles podem ser úteis e inofensivos para os usuários em geral, mas também podem ser usados de forma abusiva por criminosos. Segundo pesquisa da Imperva, em

uma ideia da abrangência e utilização desses *bots* no tráfego da internet e, em especial nas redes sociais, de acordo com uma pesquisa feita no ano de 2017 pela Universidade de Indiana (EUA), aproximadamente 15% do total de 330 milhões de perfis da rede social *twitter* eram compostos por *bots*.[25]

Para comprovar a preocupação da Justiça Eleitoral a respeito, em 11 de outubro de 2018 a Procuradoria-Geral Eleitoral do Ministério Público Eleitoral publicou a Instrução PGE nº 05, que diz:

> *"(...) 2) promover a responsabilização por ato de propaganda eleitoral irregular que (Código Eleitoral, arts. 242 e 243): a) crie, artificialmente, na opinião pública, estados mentais, emocionais ou passionais;*
>
> *3) promover a persecução de ilícitos eleitorais que comprometem a integridade do processo eleitoral, notadamente: a) contratar direta ou indiretamente grupo de pessoas com a finalidade especifica de emitir mensagens ou comentários na internet para ofender a honra ou atingir a imagem de candidato, partido ou coligação (Lei n° 9.504/97, art. 57-H, § 1°); b) prestar serviços relativos à emissão de mensagens ou comentários na internet para ofender a honra ou atingir a imagem de candidato, partido ou coligação (Lei n° 9.504/97, art. 57-H, § 2°); c) divulgar fatos que sabe inverídicos, em relação a partidos ou candidatos e capazes de exercerem influência perante o eleitorado (Código Eleitoral, art. 323);"*[26]

De acordo com dados obtidos no *website* do TSE[27], durante o período eleitoral do ano de 2018 foram protocolados 50 pedidos de obtenção de liminares para retirada de conteúdo da internet. A utilização de *fake news* com finalidade de prejudicar candidatos rivais, era uma séria ameaça à lisura do processo eleitoral. Antes desta tipificação penal que o artigo 326-A trouxe ao Código Eleitoral, os magistrados do TSE julgaram aspectos extremamente sensíveis e diretamente relacionados ao processo eleitoral, tais como a liberdade de expressão, direito ao livre pensamento, privacidade, honra e

2016 os *bots* corresponderam a mais de 50% do tráfego total da internet. Disponível em: https://www.techtudo.com.br/noticias/2018/07/o-que-e-bot-conheca-os-robos-que-estao-dominando-a-internet.ghtml Acesso em: 28 abr. 2020.

[25] Disponível em: https://www.techtudo.com.br/noticias/2018/07/o-que-e-bot-conheca-os-robos-que-estao-dominando-a-internet.ghtml Acesso em: 28 abr. 2020.

[26] Disponível em http://www.mpf.mp.br/pge/normativos/InstruoNormativa518PREsatuaaoeleitoral.pdf. Acesso em 31/05/2020

[27] Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2018/Novembro/tse-atuou-com-celeridade-no-julgamento-de-processos-sobre-fake-news-durante-as-eleicoes-2018 Acesso em: 13 abr. 2020.

dignidade da pessoa humana através de um complicado exercício de ponderação de princípios e direitos fundamentais.

Mas no que inova o artigo 326-A do Código Eleitoral (crime de denunciação caluniosa com finalidade eleitoral), se comparado com o art. 138 do Código Penal (crime de calúnia)? Ora, além do elemento subjetivo específico "com finalidade eleitoral", que consta no *caput*, o §3º do crime de denunciação caluniosa com finalidade eleitoral também tipifica como incorrendo no mesmo tipo penal "(...) quem, comprovadamente ciente da inocência do denunciado e com finalidade eleitoral, divulga ou propala, por qualquer meio ou forma, o ato ou fato que lhe foi falsamente atribuído". Portanto, o sujeito ativo desse delito deve, necessariamente, ter a finalidade eleitoral em sua conduta e pode, apenas, divulgar ou propalar tais atos.

A finalidade eleitoral não está relacionada com o fato de o crime ocorrer necessariamente em período eleitoral. Pode ocorrer em período anterior que também esteja relacionado ao processo eleitoral. No caso do §3º mencionado no tópico anterior, o sujeito ativo deve ter a finalidade de interferir no processo eleitoral ou pré-eleitoral, tanto na modalidade consumada como na tentada, apenando-se o sujeito ativo do delito à reclusão de até 8 anos e, se o delito for cometido de forma anônima ou se utilizando de nome ou perfil falso, há aumento de uma sexta parte.[28]

1.4) Crimes contra a Honra cometidos nas redes sociais

Em primeiro lugar, é importante frisar que a doutrina divide os crimes informáticos em dois grandes grupos. O primeiro grupo constitui o dos crimes informáticos próprios (também chamados de puros), uma vez que a conduta só poderia ocorrer em virtude da existência do ambiente digital ou informático. São eles os tipificados no artigo 154-A do Código Penal, que trata da invasão de dispositivo telemático, além do crime de interceptação informática (art. 10, da Lei 9.296/96), dentre outros. O segundo grupo são os crimes informáticos impróprios (ou impuros), cujas condutas ocorrem tanto no mundo digital e informático, como fora dele, como é o caso dos Crimes contra a Honra, tipificados nos artigos 138 a 140 do Código Penal e que, de acordo com o

[28] Disponível em: https://www.conjur.com.br/2019-jun-17/opiniao-denuncia-falsa-finalidade-eleitoral-agora-crime Acesso em: 21 abr. 2020.

art. 141, III[29], tem a sua pena aumentada em um terço.

Atualmente a internet e, em especial as redes sociais, tem sido utilizada também para atacar a reputação e a autoestima dos indivíduos. Em poucos segundos, a honra objetiva e subjetiva de uma pessoa pode ser atacada, seja imputando-lhe falsamente um crime, uma conduta ou divulgando informações que não condizem com a verdade. Devido à abrangência da internet e, em especial com o compartilhamento das postagens de forma quase que instantânea, trazem danos à honra da vítima que podem até ser irreparáveis.

Devido ao fato da falsa imputação de crime (calúnia), ofender a reputação de outrem (difamação) e a ofensa à dignidade ou ao decoro (injúria) serem considerados pelo ordenamento jurídico pátrio crimes de menor potencial ofensivo, que consequentemente fazem com que o agente da conduta delitiva pratique tais crimes na confiança que dará simples multa, ou serviços prestados à comunidade - e ainda a possiblidade de encerramento antecipado do processo através de medidas despenalizadoras (Transação Penal) – contribui para a falsa sensação de que a internet é "Terra de Ninguém" e, por consequência, o aumento vertiginoso dos crimes contra a honra praticados nas redes sociais. Além disso, a má utilização das redes sociais e o ambiente de polarização político-ideológica contribuem substancialmente para o acirramento dos ânimos nas redes e para o consequente crescimento deste tipo de delito[30].

2. Teoria da correlação entre acusação e sentença

O jurista Gustavo Badaró, em sua obra "Correlação entre acusação e sentença" (BADARÓ, 2020), define que a sentença é a síntese de um processo dialético, em que a acusação é a tese e a defesa, a antítese[31]. Principalmente em um Sistema de Processo Penal Acusatório, a regra da correlação entre a acusação e sentença deve ser vista como um instrumento da garantia dos princípios constitucionais do contraditório e ampla defesa, uma vez que, deve ser garantido às partes (tanto a defesa quanto à acusação), a possibilidade de reação a atos que lhe

[29] Art. 141, III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria;

[30] Uma pesquisa de 2018 da associação SaferNet Brasil, em parceria com o Ministério Público Federal (MPF), apontou 133.732 queixas de delitos virtuais. Entre eles, o crime contra a honra. Fonte. https://indicadores.safernet.org.br/indicadores.html. Acesso. 12 de fevereiro de 2021.

[31] BADARÓ, Gustavo. *Correlação entre acusação e sentença".* Ed. Revista dos Tribunais. 4ª edição. posição 347. 2020

sejam desfavoráveis – uma vez que, caso as partes conheçam elementos da sentença somente neste ato processual derradeiro, não lhes seria garantido contradizer ou influir na formação do convencimento do juiz.

Outro aspecto fundamentado na obra de Badaró (2020) é a identidade do objeto da acusação e da sentença, uma vez que, para ele não existem dois fatos ou objetos diversos a serem comparados, mas tão somente duas representações de um objeto único. O objeto no processo penal não seria a pretensão punitiva estatal, que seria justamente o poder do Estado de exigir daquele que delinquiu, de se submeter à sanção penal, ou de não punir aquele que é comprovadamente inocente. Esta pretensão punitiva, para Badaró, seria anterior ao próprio processo penal. Para ele, o objeto do processo penal é a pretensão processual penal[32], sendo a imputação penal o meio pelo qual se formula tal pretensão. E o objeto desta imputação penal é um fato atribuído a alguém, juridicamente relevante, e previsto em uma norma penal como crime.

No entanto, mesmo que a imputação não deva ser alterada ao longo do processo, durante *iter* processual pode aparecer novos elementos – como a produção de provas realizadas por perícia digital – que podem alterar a imputação. No caso em tela, sobre as diferentes imputações tipificadas pelos artigos 326-A (do Código Eleitoral) e o art. 138 (do Código Penal), vamos analisar o seguinte caso hipotético. Um candidato, devido à propagação de mensagens que maculam a sua honra objetiva e subjetiva, veiculadas por determinado perfil anônimo em uma rede social, entra com uma queixa-crime para responsabilização do autor das mensagens por crime de calúnia (art. 138, do CP), realizado em meio digital. No curso do processo, caso o querelante solicite que seja realizada uma perícia digital para comprovar a origem das mensagens e for evidenciado que o autor das mensagens era candidato à vaga eletiva do mesmo pleito eleitoral que o querelante disputava, mas em uma agremiação político partidária rival. Desta forma, surge um fato que precisa ser integrado à imputação penal: a finalidade eleitoral.

No exemplo ilustrado, mesmo que parte da doutrina jurídico penal considere que o fato da imputação deve permanecer imutável quando os seus elementos constitutivos, como o bem jurídico tutelado, forem os mesmos para o caso em

[32] BADARÓ, Gustavo. *Correlação entre acusação e sentença".* Ed. Revista dos Tribunais. 4ª edição. posição 1469. 2020

tela, tal concepção não se aplica. O bem jurídico tutelado pelo crime de calúnia é a honra objetiva e subjetiva da vítima, enquanto que o bem jurídico tutelado no crime de denunciação caluniosa com finalidade eleitoral (art. 326-A, §3º do Código Eleitoral) é a Administração da Justiça Eleitoral[33] – uma vez que, o agente ativo desta conduta quer, de forma caluniosa, influenciar o processo eleitoral. Ou seja, a imputação penal deve ser alterada, pois além da diferença de bem jurídico tutelado, ocorreu um fato imputado mais gravoso do que aquele que fora objeto da acusação originária.

Badaró sustenta que[34], quando ocorre a situação analisada acima, deve ser garantido à parte (no caso, à defesa), que apresente o seu contraditório e ampla defesa se defendendo dos fatos novos alegados – já que este foi penalmente relevante quanto à necessária nova imputação penal. Se não for garantido o direito ao contraditório e à ampla defesa, o querelado terá prejuízo em sua defesa.

Quando ocorre esta alteração, ainda segundo Badaró (2020), é necessário o aditamento da denúncia, cumprindo o prazo de aditamento e de oitiva da defesa, que consta no art. 384 do CPP, sob pena do acusado ser condenado por fato delituoso que não lhe foi imputado[35], abrindo a possibilidade de a sentença ser considerada nula ou inexistente. Importante destacar que, mesmo se a mudança da imputação penal garantir o direito ao contraditório e à ampla defesa da parte defensiva, mas prejudicar o exercício destes princípios e direitos pela acusação, também ocorre o prejuízo de uma das partes processuais e, logo, a sentença também deverá ser considerada nula ou inexistente.

Importante frisar que, quando ocorre a violação da regra de correlação entre acusação e sentença, de acordo com Badaró[36] a doutrina se divide entre aqueles que sustentam ser a sentença inexistente ou nula. Para aqueles que sustentam a inexistência da sentença, o ato é desprovido de eficácia jurídica. Já para os que defendem que a sentença é nula, esta produz efeitos até que outra decisão reconheça a nulidade, retirando a sua eficácia.

Por fim, se o aditamento da denúncia for rejeitado pelo juiz, permanece a imputação originária e, caso

[33] STJ. REsp 88.881/DF, 6ª Turma, Rel. Min. Luiz Vicente Cernicchiaro, DJU 13/10/1997, p. 51.653.
[34] BADARÓ, Gustavo. *Correlação entre acusação e sentença".* Ed. Revista dos Tribunais. 4ª edição. posição 3052. 2020
[35] DE LIMA, Renato Brasileiro; *Código de processo penal comentado.* ed. JusPodivm. 5ª edição. p. 1103. 2020
[36] BADARÓ, Gustavo. *Correlação entre acusação e sentença".* Ed. Revista dos Tribunais. 4ª edição. posição 3267. 2020

for recebida, será apreciado exclusivamente o fato superveniente que substituiu a imputação originária.

3. A importação da perícia digital na imputação do crime de *fake news* com finalidade eleitoral ou crime de calúnia

Para garantir a presunção de inocência, valor tão precioso para a permanência do Estado Democrático e Social de Direito, o processo penal deve conter, no mínimo, uma incerteza quanto aos fatos. A sentença do processo deve ser baseada no conjunto probatório, fundamentado em conhecimento, preciso e capaz de afastar a dúvida da imputação penal. E este conhecimento deve ser fundamentado por uma base empírica, como ensinado pelo mestre Ferrajioli (2002).

O papel da perícia digital é de suma relevância para evidenciar qual foi a conduta incorrida pelo sujeito ativo do tipo penal aqui discutido, ou seja, se ele realmente teve finalidade eleitoral.

A coleta de evidências digitais para a produção de provas dos crimes cometidos no ambiente virtual, como no caso da conduta tipificada no §3º do artigo 326-A do Código Eleitoral, é fundamental para comprovar que o sujeito ativo desse crime teve finalidade eleitoral ao incorrer na conduta de divulgar ou propalar (núcleo do tipo do §3º) as chamadas *fake news* pelas redes sociais, na internet.

Os vestígios nos crimes cometidos no ambiente virtual têm a particularidade de não serem percebidos pelo observador leigo no tema que, na maioria das vezes, observará tão somente o resultado da conduta. Mesmo que o objetivo aqui não seja aprofundar o desenvolvimento do tema relacionado às Ciências da Engenharia de Computação ou de Dados, é salutar elucidar conceitos básicos para que o leitor leigo consiga seguir no entendimento do assunto que será tratado.

3.1. A natureza da prova digital

A prova digital, devido à sua natureza volátil formada por combinações informáticas binárias, é mais suscetível de ser objeto de adulteração do que as provas convencionais (as cometidas nos delitos do mundo "físico"). Da mesma forma em que ela é obtida, pode ser alterada ou destruída com velocidade semelhante. Sendo assim, é de extrema importância a realização da cadeia de custódia, bem como da realização de uma perícia por profissional qualificado.

Devido às características de imaterialidade, seria recomendável que a

prova digital tivesse uma regulamentação autônoma. No entanto, essa não foi a escolha do legislador brasileiro, então a prova digital deve ser analisada com base na analogia e interpretação extensiva às demais provas materiais.

Um dos conceitos essenciais, e que fazem parte da imaterialidade física da prova digital, é que ela ocorre no ambiente digital. Este deve ser categorizado como o espaço que, para ser perceptível ao indivíduo, requer impulsos elétricos que geram dados informáticos criados, processados, armazenados e identificáveis em sistemas informáticos binários.

3.2. Classificação da prova digital

A prova digital possui uma classificação que segrega o meio em que a mensagem é trafegada e obtida, quem a produz ou a transmite e qual o seu conteúdo. Existem, basicamente, três tipos de dados e são eles: 1) dados cadastrais: aqueles a partir dos quais é possível obter informações pessoais quanto ao(s)s usuário(s) de *devices* ou de rede. Informações como nome, endereço residencial, número de série do equipamento e do IP de rede; 2) dados de tráfego: aqueles originados pela relação do usuário da rede com o provedor de acesso à internet. Geralmente, são constituídos pelos dados de obtenção de informação e contribuem para a localização dos equipamentos utilizados no delito através dos "dados de localização"; 3) dados de conteúdo: aqueles relacionados ao teor da comunicação e mensagem trocada pelo acusado e sua vítima.

Um fator determinante para a prova digital é que os elementos que vão constituí-la nem sempre ocorrem no mesmo espaço de tempo, mas antes em fases distintas da comunicação. Basicamente, existem quatro momentos em que ocorrem as etapas da comunicação telemática. A fase prévia, em que devem ser estabelecidos os elementos relacionados aos dados cadastrais do usuário da rede. Eles se estabelecem previamente, pois são necessários para estabelecer a comunicação telemática, uma vez que sem eles é impossível a efetiva utilização dos serviços telemáticos. Na segunda e terceira etapas da comunicação, que são respectivamente o estabelecimento da comunicação e a troca de mensagens e conteúdo, são de fundamental importância os elementos relacionados aos dados de tráfego e de conteúdo. Nessas etapas têm início a comunicação telemática.

Em uma investigação criminal de um delito que ocorreu em ambiente virtual, ou seja, através da utilização da

internet, um dos principais elementos que formam a prova digital é o número de endereço IP (*Internet Protocol*). O número de IP é constituído por uma sequência numérica fornecida pelo prestador de serviço de acesso à internet ao seu cliente. Funciona como uma espécie de porta de entrada do usuário na internet e as empresas que prestam serviços de conexão à internet sabem quais endereços de IP seus clientes utilizam[37]. Esse controle é fundamental para que, em uma investigação, possa ser realizada a subsunção do delito informático, identificando o possível usuário de determinado número de IP identificado pelo perito oficial como sendo o do acusado. Mas o grande desafio é a existência do chamado "IP dinâmico". Devido à grande utilidade da internet nos últimos anos (e a tendência é que essa utilização aumente), houve uma saturação de números de IPv4. Atualmente, nem todo o ecossistema da internet está preparado para a utilização do IPv6, que aumentará consideravelmente a utilização dos números de IP (apenas para ilustrar, é um conceito semelhante como o que ocorreu recentemente na telefonia celular, em que foi introduzido o nono digito devido ao fato do esgotamento das numerações de celular). Em apertada síntese, o conceito de "IP dinâmico" se traduz pelo fato de as prestadoras de serviço de conexão à internet terem fragmentado o endereço de IP em várias "portas lógicas."

Apesar do fato de o endereço de IP ser justamente concebido para utilização individual, o compartilhamento de IP através do emprego da porta lógica torna possível a individualização da navegação na internet – mesmo que mais de um dispositivo estejam conectados simultaneamente na mesma rede. Inclusive, em recente decisão da Terceira Turma do Superior Tribunal de Justiça (STJ)[38] decidiu que as empresas provedoras de aplicação da internet (como os buscadores *on-line* e redes sociais) devem ser responsáveis pelo fornecimento dos dados da porta lógica de origem para que, ao cruzar os dados desta porta com os números de IP dinâmico e os dados do usuário, seja possível individualizar o acesso a determinado conteúdo na internet. Assim, através de uma perícia seguindo os padrões da cadeia de custódia

[37] Não serão aprofundados conceitos como o esgotamento atual no número de IPv4 e a necessidade de ser implantado o endereçamento de IPv6. O objetivo é demonstrar apenas como os elementos que compõe a sistemática de acesso à internet são tratados no âmbito da prova digital.

[38] Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Provedor-deve-fornecer-porta-logica-para-identificar-usuario-acusado-de-atividade-irregular-na-internet.aspx Acesso em: 25 abr. 2020.

da prova digital, é possível identificar a conduta e o seu sujeito ativo.

3.3. Características da prova digital

As características da prova digital são: 1) imaterialidade; 2) volatilidade e fragilidade; 3) alta capacidade de dispersão e perda. Vamos analisar, com mais propriedade, cada uma dessas características.

Sobre a imaterialidade, as informações que resultam na materialidade da conduta criminosa são compostas pelo sistema binário informático. *Mutatis mutandis*, diferentemente de uma necropsia, ao abrir fisicamente um computador, não haverá uma materialidade direta do delito informático. Logo, as informações relacionadas à materialidade do crime informático serão resultado do processo de leitura eletrônica dos dados que estão armazenados nos componentes eletrônicos do computador – pois a materialidade da prova digital é composta de *bits*[39].

Devido à ausência de um critério material, a prova digital faz com que ela seja volátil e frágil. Se for manipulada sem os devidos cuidados necessários na preservação da cadeia de custódia da prova, constantes nos manuais de boas práticas, a prova digital pode ter a sua validade comprometida – ou até mesmo desaparecer. Sua manipulação pode, facilmente, alterar dados e comprometer a licitude das informações. A volatilidade e fragilidade das provas digitais são comprovadas até no momento de seu acesso. Se as técnicas de metodologia não forem seguidas, desde a coleta até a fase da posterior preservação, pode haver o comprometimento da validade da prova.

Outra característica da prova digital é a sua facilidade de dispersão. As informações sobre um mesmo delito informático podem estar dispersadas em vários compartimentos lógicos diferentes. Ou seja, devido à sua volatilidade, a prova digital pode ser fragmentada e separada em locais diferentes no mesmo sistema operacional. Mas a dispersão pode ser inclusive geográfica, uma vez que os arquivos podem ser fragmentados e dispersados em várias localidades geográficas diferentes. Os próprios servidores onde as informações estão localizadas podem estar em países diferentes daqueles em que o delito ocorreu, uma possibilidade bem grande de ser verificada nos casos concretos.

[39] Disponível em: http://producao.virtual.ufpb.br/books/camyle/introducao-a-computacao-livro/livro/livro.chunked/ch02s01.html Acesso em: 21 abr. 2020.

3.4. Cadeia de custódia da prova digital

Devido às características da prova digital mencionadas, é de extrema importância a observância da metodologia científica da cadeia de custódia da prova para a manutenção de suas condições originais e validade.

A boa prática internacional, em especial as determinadas pela *ENISA* (Agência Europeia para a Segurança em Redes e da Informação - *European Union Agency of Network and Information Security*, sigla em inglês)[40], orienta que a recolha da prova digital deve seguir cinco princípios: 1) integridade dos dados; 2) cadeia de custódia da prova; 3) apoio especializado; 4) treino apropriado e; 5) princípio da legalidade.

3.4.1. Integridade dos dados

A integridade dos dados é de extrema importância na prova digital para que se possa garantir que as informações (vestígios, evidências, dados, documentos) não foram alteradas ou deletadas. Deve-se manter a integridade dos dados em sua configuração original durante todo o curso processual do caso concreto.

3.4.2. Cadeia de custódia

Em linhas gerais, a cadeia de custódia da prova, para o conjunto dos elementos probatórios, tem papel central para a preservação das informações coletadas na fase de instrução processual. Cabe à cadeia de custódia da prova assegurar, através de documentos, a cronologia dos vestígios obtidos na perícia oficial, bem como o controle do seu acesso. Esta última característica também envolve o acesso do vestígio enquanto este estava sob a guarda e custódia da autoridade da polícia judiciária – ou mesmo de um particular.

Para tanto, também colabora a Norma Brasileira - ABNT NBR ISSO/IEC 27037[41], cujo teor versa sobre diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Trata-se de uma metodologia para obter evidência digital aceitável em processos judiciais e disciplinares. São métodos utilizados mundialmente que preservam a integridade e a autenticidade das

[40] Disponível em: https://www.enisa.europa.eu/ Acesso em: 25 abr. 2020.

[41] Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=307273 Acesso em: 25 abr. 2020.

evidências digitais. Importante destacar que a metodologia dessa norma abriga apenas as evidências que já estão no formato digital e não aquelas que estão no formato analógico e que precisam ser digitalizadas. Inclusive, mesmo na fase da investigação criminal, a referida norma pode ser utilizada como uma diretriz prática.

Por coleta entende-se como o processo de recolhimento de itens físicos com potencial de conter alguma evidência digital. Evidência digital, por sua vez, são informações ou dados armazenados ou transmitidos em forma binária, que podem ser indicados como evidência de um delito informático. Outro fator importante na cadeia de custódia da prova são as garantias de repetibilidade e reprodutibilidade. Esta relaciona-se à propriedade de que determinado resultado pode ser obtido através de um processo realizado em ambiente diferente do que fora realizado anteriormente. Aquela relaciona-se à capacidade de condução de um processo para obter os mesmos resultados em um mesmo ambiente de teste. Ambas as características são fundamentais para a cadeia de custódia da evidência digital.

A metodologia do desenvolvimento do trabalho pericial das evidências digitais devem seguir, como uma boa prática, os fundamentos sugeridos pela NBR 27023: a) documentar todas as ações; b) determinar e aplicar um método para estabelecer a confiança e exatidão da cópia da potencial evidência digital, que deve ser comparada com a original; c) reconhecer que pode ocorrer a necessidade de a preservação da evidência digital ser, em determinados casos, intrusiva.

Além desses três fundamentos, a NBR 27023 ainda apresenta outros, como a relevância, a confiabilidade e a suficiência. A relevância está relacionada ao fato de a evidência digital precisar estar associada à investigação do delito. Através da auditoria e justificação, deve o perito descrever os procedimentos seguidos para chegar às escolhas. A confiabilidade está relacionada com o fato de os processos utilizados durante a perícia terem a repetibilidade e auditoria garantidas, pois isso será importante em uma eventual necessidade de contraprova. Por fim, a suficiência está fundamentada na premissa de que a evidência digital coletada deve ser apenas o suficiente para a adequada investigação. Se tal material for recolhido sem levar em consideração esse princípio, pode-se incorrer excessos na investigação.

Outro aspecto importantíssimo da cadeia de custódia da evidência digital

está relacionado ao seu manuseio. Para tanto, é preciso garantir a auditabilidade, justificabilidade e repetibilidade (ou reprodutibilidade).

A auditabilidade é essencial para que o assistente independente, ou a outra parte interessada autorizada, avalie as atividades desenvolvidas pela perícia oficial. Por isso, é de imprescindível a documentação de todas as ações realizadas pela perícia, a fim de garantir a avaliação independente de o método científico, a técnica e os procedimentos terem sido seguidos adequadamente.

A repetibilidade é estabelecida quando os mesmos resultados de testes são produzidos sob determinadas condições, utilizando-se os mesmos procedimentos, métodos e instrumentos. Além disso, pode ser repetido, sob as mesmas condições, a qualquer tempo depois da realização do teste original. Evidente que podem ocorrer situações em que a reprodutibilidade pode ser comprometida, como num caso de envolvimento de memória volátil[42], circunstância em que o perito deverá ter mais cuidado com o controle de qualidade do processo de aquisição da evidência digital e de sua documentação.

Por fim, a justificabilidade está relacionada ao fato de o perito ter de justificar todas as suas ações e métodos para o manuseio da evidência digital.

Desse modo, o processo de manuseio da evidência digital consiste nas etapas de identificação, coleta, aquisição e preservação das informações. Se for manuseada de forma imprópria, devido às suas características voláteis, poderá ser alterada, adulterada ou destruída – o que pode fazer com que a evidência digital fique inutilizada ou sem validade jurídica. É sempre importante o perito documentar todo o processo de manuseio, especialmente se forem necessárias ações que promovam alguma alteração inevitável.

Após todo o percurso aqui explanado, resumimos, então, a descrição dos processos de identificação, coleta, aquisição e preservação das evidências digitais.

O processo de identificação envolve a pesquisa, o reconhecimento e documentação da evidência digital. Nessa etapa, identifica-se o armazenamento da mídia digital o os dispositivos que podem conter as evidências digitais. Nesse momento, é de extrema importância que sejam priorizados os dados voláteis, evitando o seu perdimento, já que podem ser facilmente destruídos se as medidas de

[42] Memória que mantém a informação apenas enquanto o computador está ligado. Ex. memória RAM. Disponível em: https://www.origiweb.com.br/dicionario-de-tecnologia/Mem%C3%B3ria-Vol%C3%A1til Acesso em: 25 abr. 2020.

segurança não forem adotadas. Um exemplo de perdimento de dados voláteis é a remoção de uma fonte de energia de determinado dispositivo. Diferentemente, os dados não voláteis são aqueles que permanecem na mídia mesmo após a remoção da fonte de energia, por exemplo.

A próxima etapa é referente à coleta ou aquisição das evidências digitais. Após serem devidamente identificados, ocorre a remoção dos dispositivos que devem ser levados para um ambiente controlado. Os dispositivos podem estar em duas situações: ligados ou desligados, existindo procedimentos técnicos a serem seguidos pelo perito em cada um desses casos. Do contrário, compromete-se também a integridade física ou lógica da evidência digital.

A aquisição é a produção de cópia da evidência digital. Essa etapa é considerada como uma das mais sensíveis da perícia digital, devendo ser documentada de forma bem detalhada. Sua reprodutibilidade deve ser feita com o menor lapso de tempo possível – pois recomenda-se que a fonte original e cada cópia de evidência digital produzam o mesmo resultado de verificação. É necessário ao perito decidir, em sua análise de risco inicial, quais métodos de coleta e equipamentos serão utilizados, bem como o nível de volatilidade dos dados que serão coletados e, ainda, se algum dado ou informação pode ter sido comprometido. Como exemplo, determinado caso poderá conter dados voláteis, como chaves de criptografia que residam na memória ativa do dispositivo, os quais podem ser perdidos se os devidos processos e metodologia não forem seguidos – recomendando-se, ao menos, que a chave para decriptar esteja acessível.

A preservação da evidência e do dispositivo digital, que deve ter início já no processo de identificação, tem o propósito de proteger a integridade contra o risco da adulteração. O propósito de manter a cadeia de custódia é possibilitar a identificação do registro ao acesso e da movimentação da evidência e dos dispositivos digitais. A cadeia de custódia da evidência digital deve conter, no mínimo, um identificador único da evidência, quem a acessou, o tempo e o local em que tal acesso ocorreu, quem foi o responsável por ter realizado a coleta, e os motivos da verificação.

CONCLUSÃO

O objetivo desse artigo foi discorrer acerca do importante papel da perícia digital, seguindo as boas práticas e garantindo a cadeia de custódia da prova digital, para garantir a exata imputação

penal no caso de dúvidas quanto à conduta delitiva do artigo 326-A do Código Eleitoral (conhecido como crime de *fake news* com finalidade eleitoral), ou do artigo 138 do Código Penal..

Inicialmente, foi realizada uma breve análise histórica sobre a evolução do conceito da imprensa até o surgimento das redes sociais, bem como a divulgação das informações e "desinformações" alteraram e influenciaram o jogo político eleitoral. Além das eleições americanas de 2016, a ocorrência desse fenômeno foi percebida pelo Tribunal Superior Eleitoral (TSE) e pela Organização dos Estados Americanos (OEA) nas eleições brasileiras de 2018, ressaltando, nesse contexto, recente publicação da OEA, a Declaração sobre a Liberdade de Expressão e as Eleições na Era Digital.

Foram apresentadas algumas formas de condutas no crime tipificado no art. 326-A do Código Eleitoral, bem como no art. 138 do CP e de que forma a perícia digital cumpre papel vital para evidenciar qual a correta imputação penal para o caso concreto.

Por fim, foram demonstradas as etapas a serem seguidas pela perícia digital e, em especial, a cadeia de custódia para garantir a integridade da prova digital.

De fato, estamos vivendo tempos em que a internet e as redes sociais podem influenciar, de forma negativa, os processos eleitorais dos países democráticos. A inverdade ou desinformação pode abalar não somente uma campanha eleitoral, mas comprometer a integridade e até mesmo a lisura de todo o pleito.

Os países democráticos, tão pouco as Organizações Internacionais, ainda não sabem como lidar com o recente fenômeno das *fake news*. Por outro lado, a criminalização excessiva da conduta poderá ensejar consequências na liberdade de pensamento e de expressão. Uma saída possível e que foi o mote do presente artigo, é demonstrar como a perícia digital é essencial para a garantia do devido processo legal e ampla defesa, além de valorizar a rigorosa metodologia que deve ser seguida para que a evidência digital seja utilizada no processo penal.

Somente com uma perícia digital aplicada de forma estritamente profissional pode-se garantir e comprovar qual a devida imputação penal deve ser correlacionada ao caso concreto, comprovando assim a finalidade eleitoral da conduta do agente. Este é, sem dúvida, um dos maiores desafios que a nossa sociedade democrática contemporânea tem pela frente, seja para garantir a lisura

do pleito eleitoral, seja para garantir o princípio da presunção de inocência, o devido processo legal e ampla defesa.

O direito deve, inequivocamente, ser o orientador dos avanços democráticos. A sociedade da informação deve continuar seu caminhar, pois não há espaço para retrocessos. Com efeito, o Estado Democrático e Social de Direito não deve ficar à mercê do dissabor dos *bots* e da "desinformação". E claro, sem jamais censurar a liberdade de pensamento e de expressão.

REFERÊNCIAS

BADARÓ, Gustavo. *Correlação entre acusação e sentença".* Ed. RT 4ª edição. 2020

BARRETO, Alecsandro Gonçalves. *Investigação digital em fontes abertas.* 2 ed. São Paulo: Brasport, 2017.

COLI, Maciel. *Cibercrimes:* limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba-PR: Juruá, 2010.

FINCATO, Denise. *Direito e tecnologia*: reflexões sociojurídicas. Porto Alegre-RS: Livraria do Advogado, 2014.

JORGE, Higor Vinicius Nogueira. *Investigação criminal tecnológica.* Vol 1 e 2. São Paulo: Brasport, 2019.

KIST, Dario José. *Prova digital no processo penal.* São Paulo: JH Mizuno, 2019,

LIMA, Renato Brasileiro. *Código de Processo Penal Comentado.* 4 ed. Salvador-BA: JusPodivm, 2019.

POLICARPO, Poliana. *Cibercrimes na e-democracia.* Belo Horizonte-MG: D´Plácido, 2016,

PRADO, Geraldo. *A cadeia de custódia da prova no Processo Penal*. Campinas-SP: Marcial Pontes, 2019.

VECCHIA, Evandro Dalla. *Perícia digital:* da investigação à análise forense. Campinas-SP: Millennium, 2019.

VELHO, Antonio Jesus. *Tratado de computação forense.* Campinas-SP: Millennium, 2016.