DESINFORMAÇÃO E ELEIÇÕES

GUIA PRÁTICO DE INVESTIGAÇÃO NA INTERNET

MPF
Ministério Público Federal
Procuradoria Regional Eleitoral no Rio de Janeiro
2020

MPF Ministério Público Federal | Procuradoria Regional Eleitoral no Rio de Janeiro

MINISTÉRIO PÚBLICO FEDERAL

Procurador-Geral da República
Antônio Augusto Brandão de Aras

Vice-Procurador-Geral da República
Humberto Jacques de Medeiros

Vice-Procurador-Geral Eleitoral
Renato Brill de Goes

Ouvidor-Geral do Ministério Público Federal
Juliano Baiocchi Villa-Verde de Carvalho

Corregedora-Geral do Ministério Público Federal
Elizeta Maria de Paiva Ramos

Secretário-Geral
Eitel Santiago de Brito Pereira

PROCURADORIA REGIONAL ELEITORAL NO RIO DE JANEIRO

Procuradora Regional Eleitoral
Silvana Batini

Procuradora Regional Eleitoral Substituta
Neide M. C. Cardoso de Oliveira

MPF Ministério Público Federal | Procuradoria Regional Eleitoral no Rio de Janeiro

Desinformação e Eleições
Guia Prático de Investigação na Internet 2020

Realização

Procuradoria Regional Eleitoral no Rio de Janeiro

Autoras

Silvana Batini

Procuradora Regional Eleitoral no Rio de Janeiro, Professora de Direito Eleitoral da FGV Direito Rio e Doutora em Direito Público pela PUC/RJ

Neide M. C. Cardoso de Oliveira

Procuradora Regional Eleitoral Substituta no Rio de Janeiro, Coordenadora adjunta do Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do MPF e Especialista em Direitos Humanos nas Relações de Trabalho pela UFRJ

ÍNDICE

I) Contexto

Há algum tempo o mundo vem se ocupando de verdadeira avalanche informativa gerada na internet[1] e, de maneira mais evidente, nas plataformas de comunicação e redes sociais. Se o crescimento acelerado do uso dessas plataformas virtuais como "espaço público" de debate e obtenção de informações já inspirava uma preocupação regulatória[2], agora não apenas é uma realidade[3], como traz consigo o agravamento de um problema que sempre existiu, mas tomou contornos imensuráveis mais sérios: as notícias falsas (*fake news*).

É importante destacar que o fenômeno do compartilhamento de notícias falsas, distorcidas ou maliciosamente descontextualizadas já está fortemente presente no cotidiano dos indivíduos, de modo que a propagação de inverdades explícitas se tornou prática natural e, via de regra, inconsequente[4].

O reflexo das *fake news* e de sua propagação, seja de boa ou má-fé, mostra-se especialmente relevante nos processos eleitorais, por representar risco palpável à normalidade e legitimidade das eleições[5].

É importante e urgente a reflexão sobre os possíveis enquadramentos dessas condutas nos modelos típicos da lei eleitoral e sondar as possíveis respostas do ordenamento pátrio, de maneira a mitigar as suas consequências deletérias às próximas eleições.

---

1 *"Se todo conteúdo digital do mundo fosse armazenado em iPads, eles formariam uma pilha com altura igual a dois terços da distância entre a Terra e a Lua"*. **Conteúdo digital dobra a cada dois anos no mundo** (09 de abr. de 2014). Revista Exame. Disponível em: https://exame.abril.com.br/tecnologia/conteudo-digital-dobra-a-cada-dois-anos-no-mundo/. Acesso em: 12/05/2020.

2 Para mais, cf. **Neutralidade de rede no Marco Civil da Internet** (disponível em: http://pensando.mj.gov.br/marcocivil/pauta/neutralidade-de-rede-no-marco-civil-da-internet/); & MAGRANI, Eduardo. **Democracia Conectada**. Curitiba: Juruá, 2014.

3 "*E a principal fonte de informação do brasileiro hoje é o aplicativo de troca de mensagens WhatsApp, segundo o levantamento. Das 2,4 mil pessoas entrevistadas, 79% disseram sempre utilizar essa rede social para se informar.*" **Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado** (12 de dez. de 2019). Agência Senado.

4 *"Uma pesquisa do Instituto Tecnológico de Massachusets (MIT), realizada de 2006 a 2017, sobre um universo de 126 mil tuítes em cascata, compartilhada 4,5 milhões de vezes no site de mensagens instantâneas Twitter, também apontou os motivos que levam uma notícia falsa a ser largamente disseminada. Segundo o estudo, o caráter 'emocionante" desse tipo de conteúdo, que não tem qualquer compromisso com a verdade, faz com que suas chances de compartilhamento sejam de 70% maiores do que as notícias verdadeiras – independentemente de seu teor, pode ser algo sobre a cura do câncer com um milagroso chá ou a morte repentina de uma celebridade que, ao contrário, vive e passa bem."*. Trecho do editorial do jornalista Tiago Sales, no artigo "O Combate às Fake News Em nome da verdade, edição da Revista Justiça e Cidadania, abril/2018.

5 Para mais, cf. **Impacto das fake news em eleições mundiais é discutido durante seminário no TSE** (17 de mai. de 2019). Tribunal Superior Eleitoral. Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2019/Maio/impacto-das-fake-news-em-eleicoes-mundiais-e-discutido-durante-seminario-no-tse. Acesso em: 12/05/2020.

II) O problema da terminologia

Embora a expressão "*fake news*" tenha ganhado popularidade, acreditamos ser melhor não utilizá-la no âmbito jurídico processual. Trabalhamos, em direito eleitoral com a necessidade de fazer exercícios de subsunção e o fato é que o termo *fake news* não expressa toda a complexidade do fenômeno e sua conformação no ambiente eleitoral. Apegar-se ao termo que remete sempre a algo falso pode levar a dificuldades na hora do eventual enquadramento de alguma conduta em ilícitos eleitorais.

Nem sempre o que circula nas redes será necessariamente falso, no sentido estrito do termo. Há hipóteses de mensagens descontextualizadas, alteradas parcialmente, ou até matérias jornalísticas em que a chamada não corresponde ao conteúdo da matéria, que pode até ser verdadeiro. É certo que em todas essas hipóteses a verdade está sendo golpeada de uma ou outra forma. Ainda assim, o emprego da expressão em contextos de interpretação literal pode conduzir a juízos ineficazes. Por outro lado, o uso da expressão *fake news* de forma indiscriminada, para desacreditar informações que circulam em redes amplia o espectro de enquadramento e igualmente pode incentivar juízos extremamente intervencionistas.

Em síntese, na ausência de um conceito jurídico preciso do que sejam *fake news*, é preciso evitar uma apreensão ilimitada ou muito restrita do fenômeno (é preciso evitar a polarização entre: tudo será *fake news* ou nada o será). Aconselhamos o emprego, por parte dos Promotores Eleitorais, em suas peças e manifestações, da expressão "desinformação", cujo significado abrange uma gama mais ampla de situações potencialmente típicas. Mesmo porque este foi o termo adotado pelo próprio TSE na Resolução 23.610/2019.[6]

III) Impactos no contexto eleitoral

No cenário em que o cidadão não apenas se informa pelas redes sociais, mas também se posiciona ativamente na internet, compartilhando opiniões e manifestando sua aprovação ou desaprovação sobre conteúdos políticos, o descontrole sobre notícias falsas é preocupante. Não há resposta fácil no complexo mundo digital.

No Estado Democrático de Direito e especialmente na seara eleitoral, a liberdade de expressão é corolário fundamental para a manutenção da democracia. É justamente com base nesse pilar que o Supremo Tribunal Federal entendeu ser inconstitucional a antiga Lei de

6 "*Seção II - Da Desinformação na Propaganda Eleitoral*". Resolução TSE nº 23.610/2019.

Imprensa (Lei nº 5.250/67) – editada em plena ditadura militar – e assentou que: *"Não existe lugar para sacrificar a liberdade de expressão no plano das instituições que regem a vida das sociedades democráticas."*[7].

Por mais que as redes sociais tenham, de fato, se tornado espaços de debate coletivo, elas não deixaram de ser plataformas privadas. Nesta condição, as empresas que sustentam as plataformas já têm adotado práticas de auto-contenção da desinformação, seja para o caso específico das eleições[8], seja para outros temas, como o caso da pandemia do novo coronavírus[9]. No entanto, a identificação dos autores e propagadores das notícias falsas, bem como a definição do filtro que determina o que deve ou não ser retirado são ainda ineficientes. Sobre o ponto, podemos destacar que há diversas formas (evidentemente não exaustivas) de explorar essa propagação de inverdades de modo a impactar o eleitorado: os próprios candidatos/partidos podem criar informações falsas; o serviço pode ser terceirizado e apenas impulsionado por ordem dos atores políticos[10]; ou isso tudo pode surgir de maneira "natural", motivado por brincadeiras ou até interesses ideológicos de eleitores inconsequentes.

Tratando especificamente dos regramentos eleitorais, é preciso reconhecer que a lei não exige de nenhum candidato um compromisso total com a sinceridade. A verdade no processo eleitoral é um valor de certa forma relativizado, já que não se espera que um candidato seja totalmente autêntico – tenderá sempre a exacerbar suas qualidades, exagerar nas suas promessas, explorar as deficiências dos adversários. O livre debate democrático convive com esse espaço de insinceridade, próprio da retórica da publicidade eleitoreira. A divulgação de boatos e mentiras, ou a exploração de vulnerabilidades dos adversários, através do emprego do exagero e da malícia, não são estratégias novas na seara eleitoral. A divulgação de histórias fantasiosas ou exageradas em desfavor de adversário tampouco é fenômeno novo. O direito eleitoral já o enfrentou diversas vezes e há ferramentas processuais tradicionais, mais ou menos eficazes para tanto, como os institutos do direito de resposta, as

---

7 Cf. **Supremo julga Lei de Imprensa incompatível com a Constituição Federal** (30 de abr. de 2009). Notícias STF. Disponível em: http://www.stf.jus.br/portal/cms/vernoticiadetalhe.asp?idconteudo=107402_ Acesso em: 13/05/2020.

8 **TSE reúne-se com Google, Facebook, WhatsApp e Twitter para alinhar estratégias de combate à desinformação nas Eleições 2020** (12 de dez. de 2019). Tribunal Superior Eleitoral. Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2019/Novembro/tse-se-reune-com-google-facebook-whatsapp-e-twitter-para-alinhar-estrategias-de-combate-a-desinformacao-nas-eleicoes-2020. Acesso em: 13/05/2020.

9 **O que as redes sociais fazem para coibir fake news em meio à pandemia** (16 de mar. de 2020). Jornal Nexo. Disponível em: https://www.nexojornal.com.br/expresso/2020/03/16/O-que-as-redes-sociais-fazem-para-coibir-fake-news-em-meio-%C3%A0-pandemia_ Acesso em: 13/05/2020.

10 Aqui se insere a figura dos "robôs", objeto de diversas propostas legislativas, cf. Uso de robôs para influenciar eleições está na pauta da CCJ (17 de fev. de 2020). Agência Senado. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/02/17/uso-de-robos-para-influenciar-eleicoes-esta-na-pauta-da-ccj Acesso em: 13/05/2020.

sanções pecuniárias e as imputações de abuso, por exemplo.

Ainda assim, há algo de inédito no contexto atual de desinformação nas eleições. E está menos ligado ao comportamento, e mais ao método e alcance. O que é novo, atualmente, é o emprego maciço desse tipo de expediente e a escala industrial e profissional que essa estratégia alcança, quando empregada através das ferramentas da internet. É a escala que transforma um artifício antigo em algo novo e desafiador. É a profissionalização e intensificação da estratégia que muda sua feição e a transforma, de expediente relativamente tolerável, em algo mais grave a ser coibido.

Vamos circular por uma zona difícil e sombreada. O pretexto de combater a desinformação nas eleições não pode autorizar o engessamento do debate e a limitação da liberdade de expressão. Aquele espaço de inautenticidade continua a existir e pretender regulá-lo completamente parece ser uma tarefa tão desnecessária quanto ineficiente, dada a dinâmica da internet. Ao mesmo tempo, a garantia da liberdade de expressão e do livre debate democrático não podem servir de salvo conduto para manobras extremamente desleais e fraudulentas que possam comprometer a normalidade e a legitimidade das eleições, valores tutelados pela Constituição.

A própria Resolução nº 23.610/2019 do TSE adverte no artigo 38:

> ***Art. 38***. *A atuação da Justiça Eleitoral em relação a conteúdos divulgados na internet deve ser realizada com a menor interferência possível no debate democrático. (Lei nº 9.504/1997, art. 57-J)*

O que o sistema de justiça eleitoral precisa, portanto, é da construção de critérios mais seguros de enquadramento típico dessas condutas. Caminhar para definir parâmetros, gerar segurança ao intérprete e desestímulo aos comportamentos notoriamente desviantes, preservando a liberdade de expressão e a natureza libertária do ambiente da internet: esse é o desafio de todos os atores do sistema de justiça eleitoral.

IV) Respostas possíveis ao fenômeno da desinformação em eleições

A legislação ordinária e as competências normativas do TSE não foram capazes de acompanhar satisfatoriamente as novas faces e transformações da desinformação em redes sociais.

A transposição pura e simples dos conceitos e limites construídos sobre a realidade

das disputas eleitorais travadas em mídias convencionais (rádio, TV e imprensa escrita) parece não ser o caminho mais adequado. Tudo mudou. O instituto do direito de resposta, de razoável eficácia nas infrações cometidas pela TV, rádio ou jornal, é menos eficaz em plataformas sociais, que não garantem a chance ao candidato de resposta ao público que foi alvo das informações falsas.

A questão precisa ser compreendida em sua complexidade fenomenológica. Qualquer tentativa de simplificação reducionaista – *fake news* é crime / *fake news* enseja direito de resposta / *fake news* é abuso / *fake news* é legítimo / *fake news* tem que ser retirado por decisão judicial - conduzirá a resultados com grande chance de erro, injustiça ou ineficácia.

De início é preciso fazer um reconhecimento humilde das limitações das vias judiciais de controle desse fenômeno. A desinformação é um desafio imposto ao mundo atual. A desinformação nas eleições tem implicações transversais e não será superada exclusivamente pelo Direito, ou pela judicialização pura e simples do problema. Não podemos criar a expectativa na sociedade de que o MPE ou mesmo a justiça eleitoral detêm a chave para coibir toda espécie de abuso que surgir nesse contexto. Temos algumas ferramentas, precisaremos lançar mão delas com inteligência e estratégia, mas elas serão sempre insuficientes.

O próprio TSE vem reconhecendo regularmente essas limitações e abrindo o diálogo institucional com as plataformas e provedores para que invistam na construção de produtos inibidores desses abusos, tais como filtros e estruturas de vigilância. São alternativas preventivas, que tentam garantir um ambiente virtual menos contaminado[11].

Prevenir a disseminação de desinformação nas eleições será sempre preferível a qualquer medida de caráter sancionatório. Mesmo porque, no ambiente virtual, uma vez que a inverdade esteja disseminada, o estrago estará feito. Mais que isso, o risco de interferência deletéria no debate eleitoral é real e é preciso evitar que a atuação judicial se transmude em censura.

Na ponta, as Promotorias Eleitorais precisarão manter a interface de diálogo com as representações dessas empresas, com agilidade e objetividade. As ferramentas de *fact checking* também precisam ser buscadas. Diálogos com as empresas e *pools* já em atividade e o treinamento de servidores nessas tarefas são necessários. O *fact checking*, como iniciativa da sociedade civil, é uma ferramenta importante de enfrentamento do fenômeno e no período

11 Neste sentido a criação, pelo TSE, do Programa de Enfrentamento à Desinformação, que hoje conta com 49 parceiros e é distribuído em seis eixos temáticos: "Organização interna", "Alfabetização Midiática e Informacional", "Contenção à Desinformação", "Identificação e Checagem de Desinformação", "Aperfeiçoamento do Ordenamento Jurídico" e "Aperfeiçoamento de Recursos Tecnológicos". http://www.tse.jus.br/imprensa/noticias-tse/2020/Maio/programa-de-enfrentamento-a-desinformacao-com-foco-nas-eleicoes-2020-mobiliza-instituicoes , visitado em 25/05/2020.

eleitoral pode vir a ter algum alcance na desconstrução de boatos e congêneres. [12]

Além disso, a checagem feita por empresas reconhecidas pode ser fonte de prova importante na caracterização da materialidade do ilícito eleitoral que esteja sendo tratado pelo Promotor Eleitoral.

V) Desinformação e ilícito eleitoral – enquadramentos possíveis

A desinformação não gera, necessariamente, uma ilicitude eleitoral. Isso porque muitas vezes a linha é tênue entre o exagero permitido pelo marketing eleitoral, a mentira desleal e a informação distorcida de forma abusiva.

Além disso, há a questão de embate entre direitos fundamentais, conforme já apontado. O art. 220 da Constituição Federal dispõe: "A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição".

Candidatos, apoiadores e adversários estão protegidos por esse direito.

Outro ponto que também vale destacar é a dificuldade, muitas vezes, de identificar aquilo que é explicitamente uma mentira. É comum que existam versões diferentes sobre um mesmo fato, sendo muitas vezes difícil determinar aquilo que seria a verdade. Embora o aprofundamento de tal questão não seja o foco deste documento, é necessário apontar para a imensa dificuldade em abordar a questão que ultrapassa os limites do direito e da ciência política, indo beber nas fontes da filosofia. Ainda assim, cabe notar que a legislação eleitoral brasileira protege, sim, um núcleo específico da verdade.

Para nós, nos estritos limites desse documento, que tem uma finalidade prática, cabe buscar e apontar quais são as alternativas concretas no tratamento da questão, diante do arcabouço jurídico e da proteção deste núcleo específico da verdade.

V.1) A via criminal

O emprego de desinformação em propaganda eleitoral pode atrair a resposta penal em diversas frentes. É uma alternativa que sabemos difícil, lenta e com baixa eficácia na proteção

12 Nesse sentido, Fernando Gallo, gerente de políticas públicas do Twitter no Brasil disse: "O poder público não pode decidir o que é verdade e o que não é. O que tem que ser feito é um processo em que a sociedade tome controle disso, de certa maneira. Tem que se buscar mecanismos para que ela consiga coibir abusos nas redes" https://politica.estadao.com.br/noticias/geral,combate-as-fake-news-deve-incluir-sociedade,70003000272.

do processo eleitoral em si, já que a dinâmica do processo penal é muito diversa da velocidade das eleições. E a via criminal eleitoral, ensina a experiência, não chega a criar um desestímulo concreto à perpetração das condutas ilícitas.

Ainda assim, a via criminal de enquadramento de determinadas condutas de desinformação nas eleições não deve ser descartada, especialmente na forma de abertura de investigações, logo que os elementos suspeitos surgirem. Se, por um lado, a vertente criminal é mais espinhosa por conta das exigências de subsunção típica e demonstração de dolo, pode significar no futuro, a única alternativa à impunidade total de determinadas condutas, já que as ações eleitorais em sentido estrito se submetem a prazos decadenciais rígidos e insuperáveis. Também porque as ferramentas da investigação criminal prestam-se com mais eficiência a determinadas diligências investigatórias e cautelares que podem vir a ser necessárias, como quebras de sigilo, cooperação internacional e até mesmo prisões.

Isto em mente, necessário remarcar que, em geral, divulgar boatos não é um ato criminoso. Porém, a lei prevê alguns casos onde a divulgação de boatos e/ou mentiras configura crime. Estes casos seriam o de calúnia [13];, a difamação[14] e a injúria eleitoral[15], crimes que se encontram no mesmo espectro de tutela do direito penal comum, protegendo a reputação alheia.

A lei ainda pune, também criminalmente, a divulgação de fato "sabidamente inverídico" na propaganda eleitoral[16]. Este último tipo, ao contrário dos crimes contra a honra, tutela o ambiente de lealdade da propaganda, além de exigir a demonstração de dolo direto (fatos que sabe inverídicos) e a difícil demonstração da potencialidade lesiva (fatos capazes de exercerem influência perante o eleitorado). Nesse ponto, é importante sustentar que não se trata de crime de perigo concreto, exigindo-se apenas a demonstração de que a

---

13 Código Eleitoral - Art. 324. Caluniar alguém, na propaganda eleitoral, ou visando fins de propaganda, imputando-lhe falsamente fato definido como crime: Pena - detenção de seis meses a dois anos, e pagamento de 10 a 40 dias-multa. § 1° Nas mesmas penas incorre quem, sabendo falsa a imputação, a propala ou divulga. §2º A prova da verdade do fato imputado exclui o crime, mas não é admitida: I - se, constituindo o fato imputado crime de ação privada, o ofendido, não foi condenado por sentença irrecorrível; II - se o fato é imputado ao Presidente da República ou chefe de governo estrangeiro; III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

14 Código Eleitoral - Art. 325. Difamar alguém, na propaganda eleitoral, ou visando a fins de propaganda, imputando-lhe fato ofensivo à sua reputação: Pena - detenção de três meses a um ano, e pagamento de 5 a 30 dias-multa. Parágrafo único. A exceção da verdade somente se admite se ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

15 Código Eleitoral - Art. 326. Injuriar alguém, na propaganda eleitoral, ou visando a fins de propaganda, ofendendo-lhe a dignidade ou o decôro: Pena - detenção até seis meses, ou pagamento de 30 a 60 dias-multa. § 1º O juiz pode deixar de aplicar a pena: I - se o ofendido, de forma reprovável, provocou diretamente a injúria; II - no caso de retorsão imediata, que consista em outra injúria.

16 Código Eleitoral: Art. 323. Divulgar, na propaganda, fatos que sabe inveridicos, em relação a partidos ou candidatos e capazes de exercerem influência perante o eleitorado:
Pena - detenção de dois meses a um ano, ou pagamento de 120 a 150 dias-multa.
Parágrafo único. A pena é agravada se o crime é cometido pela imprensa, rádio ou televisão.

conduta tem aptidão para influenciar o pleito. Essa demonstração, ademais, não está vinculada ao resultado obtido nas urnas[17], mas deve prender-se à gravidade concreta da conduta.

No caso de disseminação de desinformação pela internet, deve-se ter em conta, por exemplo, o meio empregado, o alcance que atingiu em termos de visualizações e compartilhamentos, tendo-se como referência o eleitorado local, além é claro do tipo de informação veiculada e seu grau de credibilidade em relação ao usuário médio de internet.

Há ainda outros tipos penais que podem oferecer uma moldura possível para as condutas de desinformação nas eleições, se tomarmos como referência a experiência dos últimos pleitos. Cite-se, como exemplo o artigo 57-H, §§ 1º e 2º da Lei 9504/97[18]. Sobre esses tipos, diga-se da dificuldade de sua configuração material, já que a lei alude à contratação de grupo de pessoas, sem definir o que entende por "grupo" (2, 3 ou mais pessoas), além da elementar relativa à contratação exclusivamente para a finalidade da disseminação fraudulenta da propaganda, restrição que deixa de fora uma gama enorme de condutas possíveis. Tome-se, como exemplo, a situação de um parlamentar que use seus assessores de gabinete para a realização da conduta. Pela literalidade do tipo, estão de fora do alcance penal.

Recente alteração legislativa criou a figura da denunciação caluniosa eleitoral, no art. 326-A do Código Eleitoral[19], que pode ser uma alternativa válida de enquadramento de determinadas condutas ligadas à disseminação de desinformação de conteúdo eleitoral. Nesse ponto, atente-se para o parágrafo 3º do dispositivo que amplia as possibilidades de autoria, ainda que se deva guardar que se trata de tipo acessório do caput, exigindo-se o dolo direto.

É interessante destacar ainda o tipo do artigo 296 do Código Eleitoral[20], tipo este pouco visitado pela jurisprudência, dada a sua baixa incidência. Todavia, o contexto atual traz

17 Cabe apontar que medir o grau de impacto da propagação de desinformação nos resultados de uma eleição é algo extremamente difícil. Nas palavras de Laura Chinchila, chefe de missão da OEA: "Medir impacto de fake news nas eleições é difícil". Matéria disponível em: https://www1.folha.uol.com.br/poder/2018/10/medir-impacto-de-fake-news-nas-eleicoes-e-dificil-diz-chefe-de-missao-da-oea.shtml

18 §1o Constitui crime a contratação direta ou indireta de grupo de pessoas com a finalidade específica de emitir mensagens ou comentários na internet para ofender a honra ou denegrir a imagem de candidato, partido ou coligação, punível com detenção de 2 (dois) a 4 (quatro) anos e multa de R$ 15.000,00 (quinze mil reais) a R$ 50.000,00 (cinquenta mil reais). § 2o Igualmente incorrem em crime, punível com detenção de 6 (seis) meses a 1 (um) ano, com alternativa de prestação de serviços à comunidade pelo mesmo período, e multa de R$ 5.000,00 (cinco mil reais) a R$ 30.000,00 (trinta mil reais), as pessoas contratadas na forma do § 1o.

19 Art. 326-A. 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.

20 Art. 296. Promover desordem que prejudique os trabalhos eleitorais; Pena - Detenção até dois meses e pagamento de 60 a 90 dias-multa.

de volta essa descrição típica, porque ela se abre a uma possibilidade concreta diversa, que demandaria, inclusive, uma alteração legislativa para readequação da pena.

As últimas eleições foram pródigas em boatos e alarmes falsos sobre fraude nas urnas eletrônicas e em alguns casos com aglomeração de pessoas indignadas nas portas das seções, causando tumulto. Apurações posteriores apontaram para uma articulação dolosa voltada a disseminar a desconfiança e a indignação nos eleitores. O tipo do artigo 296 pode, em tese, oferecer alguma resposta a essa conduta.

Não se pode perder de vista, também, a possibilidade de termos crimes comuns conexos a essas figuras típicas. Citem-se como exemplo, o crime de racismo, previsto no art. 20, § 2º, da Lei 7718/89., e eventualmente o crime de lavagem de dinheiro (Lei 9.613/97).

V.2) A via pelo controle da propaganda

A desinformação pode configurar, em tese, propaganda irregular.

Obviamente que toda e qualquer propaganda na internet está sujeita ao regramento previsto na Lei 9504/97 (artigos 57-A a 57-J) e à Resolução TSE 23.610/2019. Ali se encontram limites formais à veiculação que podem ser buscados como alternativas ao enfrentamento do conteúdo das postagens.

Sobre o controle de conteúdo, importante destacar que a referida Resolução impediu a retirada de conteúdos com base no poder de polícia, salvo se a retirada se fundamentar em falhas formais de postagem[21]. Significa dizer que se a pretensa ilicitude da postagem estiver contida na mensagem veiculada, será indispensável o devido processo, com contraditório e ampla defesa e, obviamente, fiscalização e atuação do Ministério Público.

Válido destacar ainda o disposto no artigo 242 do Código Eleitoral, que parece trazer uma abertura importante de enquadramento da desinformação como propaganda irregular. Confira-se:

> Art. 242. A propaganda, qualquer que seja a sua forma ou modalidade, mencionará sempre a legenda partidária e só poderá ser feita em língua nacional, não devendo empregar meios publicitários destinados a criar, artificialmente, na opinião pública, estados mentais, emocionais ou passionais.

21 Resolução TSE 23.610/109, art. 6º, parágrafo 2º: O poder de polícia se restringe às providências necessárias para inibir práticas ilegais, vedada a censura prévia sobre o teor dos programas e das matérias jornalísticas a serem exibidos na televisão, na rádio, na internet e na imprensa escrita (Lei nº 9.504/1997, art. 41, § 2º).

Não raro, os boatos que surgem e se propagam com velocidade no âmbito da desinformação pela internet são geradores de sentimentos como raiva, revolta ou medo. A disseminação orquestrada e maciça desse tipo de postagens em período eleitoral, a depender do grau em que isso aconteça, pode turbar a normalidade da formação da vontade popular e caracterizar, em tese, uma propaganda irregular na forma do artigo acima mencionado. É um dispositivo legal pouco utilizado, mas que merece ser reinterpretado à luz dessas novas configurações de desordem informativa.

A Constituição e a Lei 9504/97, em seu art. 58, garantem o direito de resposta contra veiculação caluniosa, difamatória, injuriosa ou sabidamente inverídica. Na propaganda eleitoral na internet é extremamente difícil concretizar tal direito, pelo fato de ser quase impossível, quando a propaganda se dá por mídias sociais, a reprodução das mesmas condições nas quais a desinformação foi difundida. É extremamente complicado fazer com que a resposta seja difundida para o mesmo público-alvo que foi exposto à desinformação[22]. A situação se agrava quando a desinformação é veiculada em ambientes como as correntes de WhatsApp, que são difundidas pelos usuários e que não criam uma rede facilmente rastreável de compartilhamento, sendo praticamente impossível identificar aqueles usuários que tiveram contato com a fonte falsa.

A Resolução 23.610 do TSE, em seu artigo 9º traz ainda um importante dispositivo na caracterização da responsabilidade pelo ilícito, que merece especial atenção, quando se trata de desinformação na eleição. Criou-se uma modalidade de responsabilidade presumida do candidato, partido e coligação por toda a informação por eles difundida. Estão comprometidos com a propagação da verdade e com a adoção de procedimentos de verificação da procedência das informações que vierem a difundir. Confira-se:

> Art. 9º. A utilização, na propaganda eleitoral, de qualquer modalidade de conteúdo, inclusive veiculado por terceiros, pressupõe que o candidato, o partido ou a coligação tenha verificado a presença de elementos que permitam concluir, com razoável segurança, pela fidedignidade da informação, sujeitando-se os responsáveis ao disposto no art. 58 da Lei nº 9.504/1997, sem prejuízo de eventual responsabilidade penal.

22 Algoritmos direcionam as informações que chegam ao usuário, criando uma bolha digital onde apenas se tem contato com aquilo que o usuário concorda. Mais sobre o assunto em: https://tab.uol.com.br/nova-bolha.

V.3) A via da cassação do registro ou do diploma

A fronteira que a Constituição e a lei tomaram para si e que está na essência de todo o regramento dos ilícitos eleitorais são as noções de abuso e da fraude. Abusar é exceder, ultrapassar um limite. Pressupõe que algo começou na esfera do lícito e dela se distanciou. Fraudar é iludir de forma ardilosa, é induzir alguém a erro.

Abusar ou fraudar, nas eleições, desequilibra a disputa, gera impactos potenciais na liberdade do voto, prejudica a transparência da disputa, compromete a lisura do pleito e coloca em risco a adesão final a seus resultados. Os abusos interferem no que se espera de uma eleição "normal". E a quebra da normalidade gera a incerteza sobre a legitimidade dos resultados. Essa constatação constitui o eixo de proteção constitucional expresso no artigo 14, § 9º da Constituição.

A Constituição se referiu expressamente à fraude, ao abuso de poder econômico e de autoridade[23]. A legislação complementar avançou para os abusos nos usos de meios de comunicação social[24]. Paralelamente, o legislador ordinário tipificou hipóteses concretas de abusos, nas condutas vedadas dos artigos 73 e seguintes, no artigo 30-A e até mesmo no 41-A, todos da Lei 9504/97.

A jurisprudência vem admitindo a ampliação das espécies de abuso[25] e avançou também para admitir toda e qualquer espécie de fraude como passível de viabilizar a cassação de mandato[26].

É nesse contexto que temos que enxergar o emprego massivo da desinformação: como mais uma espécie de abuso e/ou de fraude, subsumível, em tese, às grandes categorias de ilícitos com as quais já estamos habituados a lidar. Se tomarmos essa linha como parâmetro de atuação na seara eleitoral, retornaremos a um contexto mais familiar e mais seguro de atuação.

---

23 Constituição, Art. 14, § 9º: Lei complementar estabelecerá outros casos de inelegibilidade e os prazos de sua cessação, a fim de proteger a probidade administrativa, a moralidade para exercício de mandato considerada vida pregressa do candidato, e a normalidade e legitimidade das eleições contra a influência do poder econômico ou o abuso do exercício de função, cargo ou emprego na administração direta ou indireta.

24 LC 64/90, Art. 22.: Qualquer partido político, coligação, candidato ou Ministério Público Eleitoral poderá representar à Justiça Eleitoral, diretamente ao Corregedor-Geral ou Regional, relatando fatos e indicando provas, indícios e circunstâncias e pedir abertura de investigação judicial para apurar uso indevido, desvio ou abuso do poder econômico ou do poder de autoridade, ou utilização indevida de veículos ou meios de comunicação social, em benefício de candidato ou de partido político, obedecido o seguinte rito: (...)

25 Cite-se, como exemplo, a hipótese de abuso de poder religioso. RO nº 265308, 2017, e RO nº 537003,2018.

26 A ideia de que a expressão "fraude" contida no art. 14, § 9º da Constituição se referia tão somente à fraude da eleição propriamente dita está superada na jurisprudência há bom tempo. Vejam-se, como exemplo, as recentes decisões do TSE, admitindo a cassação de registro e diploma em casos de fraude às cotas de gênero. (TSE - RESPE: 149 - PI, 2015 e ainda RESPE Nº 0000193-92.2016.6.18.0018

A caracterização do ilícito do uso indevido dos meios de comunicação social, tradicionalmente atrelado às mídias convencionais, também merecerá um novo enfoque, a possibilitar o enquadramento típico e atuação do Ministério Público Eleitoral, para abranger a divulgação de notícias falsas pela Internet. Seja por pessoas físicas, seja quando envolverem, ainda que indiretamente, instituições religiosas, sindicatos e pessoas jurídicas em geral.

A criação de perfis falsos e a viralização artificiosa de notícias falsas configura a fraude, hipótese expressa de impugnação de mandato eletivo contida no artigo 14, § 10 da Constituição e ainda passível de ser sustentada em AIJE.

A constatação de que houve pagamento para impulsionamento indevido de postagens contendo *fake news* pode caracterizar o ilícito de abuso de poder econômico e eventualmente do artigo 30-A da Lei 9504/97 (gastos indevidos de campanha). Em ambas as hipóteses, uma vez indiciada a anuência do candidato, justifica-se a propositura da medida judicial tendente à cassação do registro ou do diploma, conforme o caso. Para tanto, será necessário instaurar o procedimento de investigação o quanto antes, para a coleta dos elementos necessários à propositura da AIJE ou da AIME.

Assim, na investigação de desinformação em processos eleitorais será importante buscar dados sobre os meios digitais que impulsionam o alcance das notícias falsas, o número de compartilhamentos e sopesar esses números em relação ao colégio eleitoral em questão.

Deve-se investigar se há emprego de perfis falsos, se há emprego de fraude nesses compartilhamentos e quem está financiando o mercado de impulsionamento artificial da desinformação.

Os impulsionamentos podem ser feitos de acordo com as políticas de uso das próprias redes sociais – o que facilita a análise de quem o fez e quanto gastou -, mas também o podem ser feitos de forma artificial, por meio de *bots*, que nada mais são do que perfis falsos criados com o único intuito de promover reações artificiais a postagens específicas para aumentar o alcance dessa publicação. Casos notórios de impulsionamento artificial acontecem no Twitter[27].

Importante lembrar que as hipóteses genéricas de abuso tem conteúdo aberto e dependerão sempre de análise de seu impacto na situação concreta. E essa análise estará, nos casos de desinformação, ligada ao contexto local da eleição e gravidade concreta do ilícito.

A caracterização do abuso ou da fraude, nesses contextos, seja de qualquer espécie, estará muito mais atrelada à forma como a disseminação da desinformação é feita do que

27 Para mais sobre bots e redes sociais, cf.: RUEDIGER, Marco Aurelio. Artigo: Os robôs nas redes sociais. FGV DAPP. Disponível em: http://dapp.fgv.br/artigo-os-robos-nas-redes-sociais/. Acesso em: 16/05/2020.

propriamente ao conteúdo disseminado. Não é dizer que o conteúdo não seja importante, mas ele deixa de ser o foco. As atenções devem ser direcionadas à identificação das estratégias de disseminação desses conteúdos que, necessariamente, resvalam para o ilícito. Em resumo, a atenção deve estar muito mais na forma de veiculação do que no conteúdo em si.

Com isso, evita-se a discussão insuperável sobre a censura e o controle da liberdade de expressão. É dizer que, para a caracterização do ilícito, deve-se velar mais pela legitimidade das condutas, do que propriamente pela autenticidade das mensagens postadas. O valor a ser tutelado nesses casos é menos a verdade e mais a lealdade da disputa.

O olhar mais vigilante sobre a forma do que sobre o conteúdo nos redireciona para um terreno em que o direito eleitoral já trafega com mais segurança e tradição. Afinal, a liberdade de expressão não protege o abuso e nem a fraude.

V.4) Como virá a desinformação nas eleições de 2020?

O potencial lesivo da desinformação nas eleições de 2018 vem sendo estudado e continua sendo objeto de análise e de perplexidades[28]. O mesmo grau de incertezas deve ser esperado para as eleições de 2020. Já se sabe que a desinformação afeta o curso das eleições, embora seja extremamente difícil calcular o real impacto no eleitorado. Porém, embora não possa ser encontrado o impacto exato, projeções podem estimar o alcance da desinformação. Estudos da FGV DAPP por exemplo identificaram as menções sobre notícias falsas no Twitter.[29]

Podemos, assim olhar para as últimas eleições a fim de tentar compreender o fenômeno e suas múltiplas faces[30], mas é impossível prever que o modelo de desinformação que prevaleceu em 2018 continuará a prevalecer em 2020. O desafio será o WhatsApp, o Instagram, o Facebook?

Espera-se que as precauções já implementadas pelos provedores de redes sociais – e já destacadas no início deste material – possam facilitar o controle e diminuir o alcance da desinformação, mas certamente não serão suficientes. O recurso do WhatsApp, por exemplo,

28 Sobre o tema, veja-se: CRUZ, Francisco Brito: Internet e Eleições no Brasil – Diagnóstico e Recomendações, 1ª. ed., 2019/2020, acessível em https://www.internetlab.org.br/wp-content/uploads/2019/09/policy-infopol-26919_4.pdf

29 http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/25742/Desinforma%c3%a7%c3%a3o%20Policy-Paper-2%20Sala.pdf?sequence=1&isAllowed=y

30 Nesse sentido, cf.: Um Brasil dividido e movido a notícias falsas: uma semana dentro de 272 grupos políticos no WhatsApp (5 de out. de 2018). BBC. Disponível em: https://www.bbc.com/portuguese/brasil-45666742. Acesso em: 16/05/2020.

de limitar a formação de grupos e de disparos pode não ser eficaz para evitar o abuso em eleições em municípios muito pequenos.

Será preciso ter atenção para todas as formas possíveis de compartilhamento disponíveis hoje no mundo virtual. Como repisamos, por mais que os meios mais utilizados até então tenham sido os encaminhamentos de mensagens por WhatsApp e postagens tradicionais no Facebook e no Instagram, será importante atentar para a desinformação em *stories*, que duram apenas 24 horas e, de maneira indireta, pelos impulsionamentos de postagens.

Por último, outro ponto que deve merecer atenção dos órgãos de fiscalização são os chamados influenciadores digitais. Como já dito, deve-se evitar, tanto quanto possível, a discussão e o enfrentamento pela via da análise do discurso/conteúdo das mensagens. O influenciador digital é alguém com liberdade plena de externar suas posições e a Constituição lhe garante esse direito. Ainda assim, a intensidade das mensagens que favorecem ou prejudicam candidatos e a pertinência dessas mensagens com o conteúdo tradicional do canal podem levantar a suspeita de que haja contratação da pessoa para a disseminação da propaganda.

Assim, no caso dos influenciadores digitais com muito destaque na localidade, é relevante investigar se houve ou não algum tipo de financiamento oculto para que fosse produzido ou divulgado conteúdo com o intuito de beneficiar (ou prejudicar) candidato e/ou partido específico, o que pode se enquadrar em gasto ilícito de campanha (Art. 30-A da Lei nº 9.504/97), ou abuso de poder de comunicação, o que demanda a instauração dos instrumentos formais de apuração.

VI) Internet

A Internet é um ambiente virtual, construído sobre uma estrutura simples, onde ocorre a transferência de pacotes de dados, de uma ponta a outra, entre redes de computadores, sem que haja descriminação sobre o conteúdo do que está sendo transmitido. E essa ausência de interferência sobre o que está sendo transmitido é que garante o que chamamos de neutralidade da rede. A Res. TSE nº 23.610/2019, art.37, inc. I definiu o conceito de Internet como "sistema constituído de conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes".

A principal característica de qualquer ato praticado em meio virtual é que ele deixa rastro. Isto porque para que um sistema informático ou para que a Internet funcione existe uma coordenação de identificadores únicos de forma que o nome e número que são digitados na barra de endereços quando fazemos uma busca, por exemplo, identificam um endereço único que permite que os computadores se encontrem, isto é, permite a difusão das informações e a entrega de dados exatamente ao destino pretendido.

Isso faz com que toda a movimentação nesse meio fique registrada, permitindo ao investigador seguir a pista e identificar os autores dessa movimentação.

No entanto, como esse funcionamento implica na geração de uma quantidade gigantesca de *bits* e *bytes*, a vida útil dessas informações não é garantida, restando preservados somente os dados relevantes ao próprio sistema, a menos que haja ordem específica para tanto. Aqui está a segunda característica dos atos, sejam delituosos ou não, praticados na Internet: as provas digitais que podem identificar o usuário são voláteis, sendo imprescindível a existência de agilidade na sua coleta.

A investigação de qualquer ato na Internet implica no conhecimento acerca da lógica do sistema informático e da própria Internet, que se sofistica conforme diferentes aplicações de internet ou sistemas passam a ficar disponíveis para utilização.

VII) A governança da Internet

É preciso fazer um pequeno parêntese para explicar como funciona a governança da Internet.

A Internet é regulada pela ICANN – Internet Corporation for Assigned Names and Numbers[31], uma entidade multissetorial, sem fins lucrativos, de âmbito internacional, onde se fazem representados governos, setor técnico e a sociedade civil, que determina os rumos da Internet. No seu início, na década de 60, era utilizada para fins militares e depois para fins acadêmicos, então controlada pelo Departamento de Comércio dos Estados Unidos. Recentemente, após o escândalo Snowden, de controle sobre os dados de usuários de Internet pela agência americana de segurança, NSA -National Security Agency, cresceu a pressão para que a ICCAN passasse ao controle de uma entidade também multissetorial, como é a natureza da Internet, sem estar vinculada a nenhum governo especialmente, sendo esse o atual modelo adotado.

31 http://archive.icann.org/tr/portuguese.html.

O que importa compreender é que a ICCAN desempenha diferentes funções como o controle de nomes e domínios, funções de administração central da rede e, a função desempenhada pela IANA[32], que é a responsável pela alocação dos *Internet Protocols* no mundo. Assim, cada região do globo recebeu um lote de IPs (*Internet Protocol*)[33] para gerir.

No Brasil, o NIC.br[34] é o braço executivo do Comitê Gestor da Internet no Brasil – CGI.br, entidade privada, que controla o .br, e é o responsável por alocar os números IP para as operadoras de telefonia que, por sua vez, disponibilizam um único número IP para cada conexão de Internet, sendo portanto possível identificar o endereço a partir de onde foi feita aquela conexão.

VIII) O esgotamento do IPv4

No princípio, o *Internet Protocol* era composto por quatro grupos de *bytes* de 32 *bits* cada, o chamado IPv4. Porém, devido à utilização crescente da Internet, com cada vez mais conexões sendo utilizadas pelo mesmo indivíduo, já que uma pessoa não representa mais somente uma conexão, mas várias. Uma só pessoa pode estar logada ao mesmo tempo no aparelho celular, no *tablet*, no *notebook*, no aparelho de TV e em uma infinidade de outros aparelhos, que apontam para o desenvolvimento da Internet das Coisas -IoT – Internet of Things, ocorreu o esgotamento do modelo IPv4.

Atualmente, muitos países (todos os desenvolvidos) já migraram para o IPv6: número

32 IANA – Internet Assigned Numbers Authority.

33 Res. TSE 23.610/2019, art. 37, inc. III - Endereço de protocolo de internet (endereço IP): o código numérico ou alfanumérico atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;.

34 No Brasil, o NIC.br – Núcleo de Informação e Coordenação do .br é o braço executivo do Comitê Gestor da Internet do Brasil – CGI.br, e é o responsável por alocar os números IP para as operadoras de telefonia que, dentre o lote de IPs a ela destinado, disponibiliza um único número IP para cada conexão de internet que algum dos seus clientes faça. A identificação do IP nessa etapa vai identificar o usuário titular daquela linha telefônica ou de banda larga, seus dados cadastrais como endereço residencial, que as companhias telefônicas ou outras têm justamente para realizarem a cobrança de seus serviços.

de *Internet Protocol* com oito grupos de *bytes* de 4 dígitos hexadecimais e 128 *bits*, cada (o quádrulo do IPv4), o que aumentou consideravelmente as possibilidades de conexões à rede.

O que temos atualmente, no Brasil, é a seguinte situação: os provedores de aplicações de internet já migraram para o IPv6, mas os provedores de conexão no Brasil, aqueles que dão o acesso à Internet, estão em fase de implantação do IPv6.

A falta de IPs disponíveis para conexões à Internet, aliada ao alto custo para a implementação do IPv6, fez com que as operadoras brasileiras de telefonia passassem a utilizar, a partir de janeiro de 2015 (com o fim dos endereços IPs na versão 4 - IPv4, brasileiros), o sistema conhecido como CGNAT-44: um sistema no qual um mesmo IP pode ser compartilhado por muitos usuários ao mesmo tempo. Seria mais ou menos como utilizar um filtro de linha, com diferentes usuários se plugando nas tomadas/entradas de um mesmo IP.

Para a identificação unívoca do usuário seria necessário que cada "tomada" fosse identificada, isto é, cada porta lógica (porta de origem) - mais um dado identificado por números, precisaria ser guardado tanto pelos provedores de conexão à internet, quanto pelos provedores de aplicações de internet, além do número de IP, data e hora, o que demanda mais investimento.

A consequência disso é que, embora os provedores de conexão de internet estejam avançando na implementação do IPv6, a maioria deles permanece utilizando o sistema NAT-44, pelo menos na telefonia móvel, e muitas investigações que dependiam somente da informação referente àquelas conexões efetuadas através do NAT 44 (os dados cadastrais de usuário do titular dos serviços da operadora) acabaram ficando sem solução, porque, eventualmente, o provedor de conexão informa que vários (centenas/milhares) clientes seus utilizaram aquele mesmo número de IP, na data e horário requisitados.

Uma forma de contornar esse problema e vem sendo utilizada é ampliar a investigação no tempo. Por exemplo, vc está investigando 4/5 postagens de um usuário, o investigador pede todos *logs* de acesso, em determinado período. E a resposta veio com diferentes IPs em datas e horas diferentes, no período solicitado. E todos esses IPs são IPv4, foram utilizados por mais de um usuário ao mesmo tempo. então se são 4/5 postagens, pode se pedir todos os endereços de conexão dessas postagens., em um período de tempo maior (se antes tinha pedido só dos últimos 6 meses, pede de um ano), se se tiver sorte, só um endereço vai aparecer nas 4 listas, um IPV6 (para o qual não existe compartilhamento), que é o do investigado.

Indico *links* de vídeos explicativos produzidos pelo NIC.br, que dão uma explicação

didática sobre o funcionamento da Internet.[35]

IX) Marco Civil da Internet

Antes da publicação do Marco Civil da Internet, as alterações da Lei nº 9.613/1998 (Lei da lavagem de dinheiro) introduzidas pela Lei nº 12.683/2012 trouxeram no artigo 17-B a possibilidade de que a autoridade policial e o Ministério Público tivessem acesso aos dados cadastrais de um investigado, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito, fazendo a primeira menção, portanto, aos dados mantidos pelos provedores de internet.

Porém, a grande inovação veio com a promulgação do Marco Civil da *Internet*, Lei nº. 12.965/2014, que estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil e, em seu bojo, regulou as questões processuais referentes à preservação das provas digitais pelos provedores, disciplinando o acesso a elas.

Assim, o artigo 11 do Marco Civil[36] estabelece que será aplicada a legislação brasileira sempre que alguma das condutas referentes ao manuseio de dados ou comunicações por provedores de conexão e de aplicações de internet ocorrer em território nacional. E seu § 2º esclarece que o *caput* se aplica mesmo que as atividades descritas sejam realizadas por pessoa jurídica sediada no exterior quando o serviço for ofertado ao público brasileiro ou ao menos uma integrante do mesmo grupo econômico possuir estabelecimento no Brasil.

O artigo 13 do Marco Civil trata da guarda e retenção dos registros de conexão à internet, que devem ser mantidos em sigilo e em ambiente controlado e de segurança, pelo prazo de um ano, podendo o Ministério Público ou as autoridades policial e administrativa

---

35 Os vídeos mais importantes são o primeiro, sobre o Protocolo IP e o quarto sobre Governança da Internet:
1.Como funciona a internet ? Parte 1: O Protocolo IP
https://www.youtube.com/watch?v=HNQD0qJ0TC4
2.Como funciona a internet ? Parte 2: Sistemas Autônomos
https://www.youtube.com/watch?v=C5qNAT_j63M&t=41s
3. Como funciona a internet ? Parte 3: DNS
https://www.youtube.com/watch?v=ACGuo26MswI
4. Como funciona a internet ? Parte 4: Governança da Internet
https://www.youtube.com/watch?v=ZYsjMEISR6E

36 Lei 12.695/2014. art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
(…)
§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

requererem cautelarmente que a guarda e preservação se dê por período superior a um ano, cabendo à autoridade requerente providenciar a autorização judicial para acesso aos dados dentro de 60 dias.

O artigo 15 do Marco Civil estabelece o dever de guarda e retenção dos registros de acesso a aplicações de internet, sob sigilo e em ambiente controlado e de segurança, pelo prazo de seis meses, também sendo facultado ao Ministério Público e às autoridades policial e administrativa requererem, cautelarmente, a preservação dos registros de acesso a aplicações por prazo superior, desde que providenciem o ingresso do pedido de autorização judicial para o acesso aos dados no mesmo prazo de 60 dias.

A importância do Marco Civil, na questão das provas digitais, está em ser a primeira lei brasileira a prever prazos de retenção e possibilidade de preservação de registros de conexão e de acesso a aplicação de internet, que são, ao mesmo tempo, meios investigativos para se buscar a identificação do usuário e também elementos probatórios para embasar a conclusão da individualização pessoal da conduta.

IX.1) Conceitos

O Marco Civil da Internet traz, em seu artigo 5º, conceitos básicos como a definição de endereço de protocolo de internet (endereço IP - *Internet Protocol Address*)[37], código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (inciso III); definição do que é registro de conexão[38]: conjunto de informações referentes à data e hora de início e término de uma conexão à internet, mediante a atribuição ou autenticação de um endereço IP (inciso VI); definição do que é registro de acesso a aplicações de internet[39]: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (inciso VIII).

O artigo 10, §1º estabelece que as informações dos provedores de conexão e de aplicação somente poderão ser obtidas por ordem judicial. Mas para autoridades, o acesso a dados cadastrais dispensa a ordem judicial.

Neste ponto é de se destacar que o regulamento do Marco Civil da Internet, Decreto nº 8.771, de 11 de maio de 2016, define dados cadastrais como filiação, endereço e qualificação

37 É um rótulo numérico atribuído a cada dispositivo (computador, celular, notebook, etc) conectado à Internet, justamente para identificar a máquina que fez a conexão à Internet. Observe que a identificação não é do usuário, mas do dispositivo.

38 Res. TSE 23.610/2019, Art. 37, inc. VI.

39 Res. TSE 23.610/2019, Art. 37, inc. VIII.

pessoal (nome, prenome, estado civil e profissão). Embora as informações financeiras não constem desse rol, é pacífica a jurisprudência no sentido de que os dados de pagamento de um serviço, seja ele por meio de conta bancária ou cartão de crédito, ou outro meio, não são protegidos pelo sigilo, de forma que os provedores tanto de conexão, quanto de aplicação de internet, devem informá-los às autoridades requerentes (polícia, Ministério Público e autoridade administrativa), independentemente, de ordem judicial.

Note-se, ainda, que no art. 13, §2º, incs. I e II do Regulamento, há a obrigação de exclusão dos dados pessoais, comunicações privadas e registros de conexão e de acesso a aplicações, após atingida a finalidade de seu uso, ou o prazo legal, se não houver solicitação de preservação por prazo superior (um ano para provedores de conexão e seis meses para provedores de aplicação).

IX.2) Prazos de Retenção e de Preservação

O Marco Civil da Internet previu prazos de retenção para os registros de conexão pelo período de um ano (art. 13) e de retenção pelo período de seis meses (art. 15), com a possibilidade de pedido de preservação por período superior a ser feito pela polícia, Ministério Público ou autoridade administrativa.

Não há obrigação de guarda/retenção de conteúdo, mas este pode ser objeto de pedido de preservação enquanto se obtém a ordem judicial para o seu fornecimento. Bastará a ordem judicial para afastar o sigilo e obter o conteúdo armazenado, nos termos do art. 7º, inciso III do MCI. Para o conteúdo *online*, isto é, para interceptação de conteúdo em tempo real, a ordem judicial deve ser na forma da lei, nos termos do art. 7º, inciso II do MCI e compreende-se que é a Lei nº 9296/96, Lei das Interceptações Telefônicas e Telemáticas, devendo, portanto, obedecer aos requisitos nela previstos.

IX.3) Jurisdição

Como já explicado acima, o artigo 11 do MCI deixa claro que se aplica a legislação brasileira para qualquer operação de tratamento de dados realizada em território nacional, devendo ser respeitados os direitos à privacidade, proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros quando pelo menos um dos terminais está localizado

no Brasil. Ou seja, a coleta de dados se deu a partir de uma conexão feita no território nacional, não importando que a sede da pessoa jurídica do provedor de aplicação de internet esteja no exterior, desde que o serviço esteja sendo ofertado ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil (ex.: a empresa WhatsApp Inc. por integrar o mesmo grupo econômico do Facebook Inc., que possui representação brasileira).

Esse dispositivo vem para assegurar que os dados do público brasileiro terão asseguradas as garantias de privacidade e segurança estipulados na lei nacional. Assim, da mesma forma para o afastamento do sigilo desses dados deve ser observada a lei brasileira, emprestando segurança quanto ao regime de proteção desses dados.

Note-se que a hipótese de oferta de serviços ao público brasileiro, sem que haja sede ou filial da empresa em território nacional, também determina a jurisdição brasileira, embora possa haver problemas para dar eficácia às decisões direcionadas a essas empresas.

Para se determinar se a oferta de serviços é direcionada ao público brasileiro, aplica-se o *targeting test* da doutrina americana, verificando-se se os serviços são oferecidos na língua portuguesa; se é possível adquirir produtos e serviços na moeda local; e se os dados recolhidos no País são utilizados para fazer publicidade direcionada a esse mesmo público. Assim, nesses casos de ofertas de serviços ao público brasileiro, esses provedores de aplicações de internet também devem cumprir a legislação brasileira.

IX.4) Sanções: Art. 12 MCI pelo Descumprimento dos Arts. 10 e 11, MCI

As sanções estipuladas para o descumprimento dos arts. 10 e 11 do MCI, sem prejuízo das demais sanções cíveis, criminais ou administrativas cabíveis, são:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II – multa de até 10% do faturamento do grupo econômico no Brasil, observando-se a condição econômica do infrator e avaliando-se a proporcionalidade entre a gravidade da fala e a intensidade da sanção;

III – suspensão temporária das atividades que envolvam os atos previstos no artigo 11;

IV – interrupção das atividades que envolvam os atos previstos no art. 11.

Logo, há o dever legal da empresa de prestar informações requisitadas por ordem judicial (brasileira), notando-se que a multa cominatória (art. 12, parágrafo único): estabelece

a solidariedade da empresa estrangeira pelo pagamento da multa cominada a sua filial, sucursal ou escritório ou estabelecimento situado no país.

Iniciou-se, no dia 27 de junho passado, o julgamento[40] da ADIN 5527, e da ADPF 403, ambas de 2016 (sobre o bloqueio do WhatsApp), no STF, cuja relatora da ADIN, Ministra Rosa Weber, entendeu sobre essas penalidades de suspensão temporária e de proibição de exercício das atividades, previstas no Marco Civil da Internet, que somente podem ser impostas aos provedores que descumprirem a legislação brasileira sobre coleta, guarda, armazenamento ou tratamento de dados. As punições, a seu ver, também são aplicáveis aos que violem os direitos da privacidade, a proteção dos dados pessoais e o sigilo das comunicações privadas e dos registros. A ministra afastou qualquer interpretação da lei que permita a punição pela inobservância de ordem judicial que determine a disponibilização de conteúdo de comunicações mediante a fragilização deliberada dos mecanismos de criptografia voltados à proteção da privacidade. O ministro Edson Fachin, relator da ADPF 403, também proferiu seu voto, no mesmo sentido da ministra Rosa Weber. O ministro Alexandre de Moraes pediu vista após o voto do Ministro Édson Fachin e o julgamento foi retirado da pauta[41].

X) Detecção de Desinformação

Boatos diversos – a checagem de informações sobre qualquer notícia passa por duas etapas: uma com a análise dos elementos da notícia e outra com a verificação do conteúdo em fontes seguras de informação.

Na primeira etapa, ao receber a notícia, verificar a linguagem usada e a aparência da mensagem. Erros de ortografia e de português, e logos de empresas conhecidas com aparência dos originais, mas com cores/fontes diversas ou outras imperfeições.

Ultrapassada a primeira etapa, consultar sites de grandes meios de comunicação e fontes oficiais relacionadas ao contudo da notícia (ex. se for sobre o processo eleitoral, o site do TSE etc) para apurar se a notícia é realmente verdadeira.

Os seguintes endereços de grandes grupos de comunicação publicam checagem periódicas de notícias:

Agência Lupa/Grupo Folha: https://piaui.folha.uol.com.br/lupa/tag/fake-news/

40 http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444265&ori=1
41 https://link.estadao.com.br/noticias/empresas,alexandre-pede-vista-e-decisao-do-stf-sobre-bloqueio-ao-whatsapp-e-adiada,70003317970

Agência Estado: https://politica.estadao.com.br/blogs/estadao-verifica/veja-todas-as-checagens-sobre-coronavirus-publicadas-pelo-estadao-verifica/

Grupo Globo: https://g1.globo.com/fato-ou-fake/noticia/2020/01/28/veja-o-que-e-fato-ou-fake-sobre-o-coronavirus.ghtml

Além disso, o *WhatsApp* disponibilizou consultas diretamente do aplicativo para checagem da veracidade de notícias no *Google* (https://www.ajudandroid.com.br/whatsapp-permite-pesquisar-google-conferir-informacoes/?amp).

Para mais informações, consulte: https://cartilha.cert.br/fasciculos/boatos/fasciculo-boatos.pdf.

Golpes por meio de promoções – além de notícias falsas, podem surgir àquelas referentes a promoções falsas, no período eleitoral (ex. oferecimento de alguma vantagem ao eleitor).

Caso haja o recebimento de *links* para promoções, aja da seguinte forma:

- Faça a checagem mencionada no item anterior;
- Verifique com o remetente do link se ele conhece a origem e pode atestar a procedência. Desconfie de correntes e links que pedem o compartilhamento com mais usuários;
- Caso o link refira-se a uma empresa, verifique no site oficial da empresa se há alguma informação sobre a promoção ou a notícia;
- Não forneça, em nenhuma hipótese, dados bancários ou senhas. Tanto bancos como empresas informam que não pedem senhas pessoais de seus clientes.
- Cartão de crédito – fornecer o número do cartão só se estiver comprando realmente algo e em lojas online confiáveis.

Não havendo confirmação por fontes seguras de que o link é verdadeiro, tratá-lo como falso: não fornecer informações pessoais e, principalmente, não compartilhar.

Dica: colocar a palavra golpe junto de eventual promoção em sites de busca para ver se outras pessoas já sofreram o mesmo golpe.

Instalação de Aplicativos que prometem informações sobre a pandemia – procure sempre o produto/empresa na loja on-line oficiais do seu sistema operacional (*Android* ou *IOS*) ou de desenvolvedores. Antes de instalar, pesquise na Internet sobre o aplicativo. Ao instalar aplicativos, evite fornecer dados e permissões desnecessários.

XI) Provas Digitais

As inovações tecnológicas tornaram essencial a preocupação com as provas digitais, pois não somente os crimes tipicamente digitais, mas todos os ilícitos praticados na Internet podem ter deixado pistas digitais e pode-se precisar dessas provas para sua elucidação.

Qualquer crime comum ou eleitoral, por exemplo, pode vir a ser solucionado com o auxílio de provas digitais. *E-mails* recebidos e enviados; pesquisas de busca sobre determinados temas na *internet;* documentos armazenados em meio digital; entre outros, podem vir a ser pistas e provas acerca do cometimento de ilícitos.

XI.1) Características

As provas digitais apresentam características intrínsecas que as tornam aptas à verificação. Elas deixam marcas, ou seja, são o próprio rastro das condutas praticadas no mundo virtual, pois toda atividade nesse ambiente deixa rastro. Pode ser verificada. Uma vez que uma informação é registrada na Internet ou em algum dispositivo informático, essa informação pode ser recuperada dentro de um certo período, mesmo que seja apagada. Assim, a perícia forense tem condição de analisar as provas digitais para verificar sua autenticidade e integridade, podendo assim determinar seu grau de confiabilidade.

Como esclarecido em estudo específico sobre o assunto[42], as provas digitais possuem requisitos específicos de validade que precisam ser observados em qualquer transferência de informações, seja ela interna ou transnacional. Deve ser primeiramente admissível, isto é, como qualquer outra prova, sua aquisição deve ser correta para que possa ser admissível. O segundo requisito, desta vez, específico à sua natureza, é que sua coleta e preservação devem ser realizadas observando-se os princípios da ciência computacional a fim de garantir sua autenticidade e integridade. Estas características podem ser verificadas na análise das provas digitais pela perícia forense que poderá determinar então o seu grau de confiabilidade. Dessa forma, a prova somente será convincente, em juízo, se bem esclarecido no laudo pericial o grau de confiabilidade dessa prova, pois na maior parte das vezes, é a prova determinante para a indicação de autoria do fato, delituoso ou não.

A perícia forense terá papel fundamental, portanto, na análise dessas provas, sendo indispensável que o perito, ou agente apto, acompanhe as ações de busca e apreensão para ga-

42 DOMINGOS, Fernanda Teixeira Souza. *As provas digitais nos delitos de pornografia infantil na internet.* IN *A Prova no enfrentamento à Macrocriminalidade*, organização DANIEL DE RESENDE SALGADO e RONALDO PINHEIRO DE QUEIROZ. Ed. JusPodivm. 2015.

rantir a correta coleta das provas digitais a fim de que nenhuma informação seja perdida ou corrompida.

Outro aspecto fundamental a ser observado é o tempo na obtenção dessas evidências, já que a prova digital é também extremamente volátil.

No dizer de Araújo Cintra, Ada Pelegrini e Cândido Dinamarco, *a prova constitui, pois, o instrumento por meio do qual se forma a convicção do juiz a respeito da ocorrência ou inocorrência dos fatos controvertidos no processo.*[43]

Dentre os meios de prova tradicionais – exame de corpo de delito e perícias em geral, interrogatório, confissão, depoimento do ofendido, prova testemunhal, reconhecimento de pessoas e coisas, acareação, prova documental, prova indiciária e busca e apreensão – podemos dizer que praticamente todos eles sofreram alguma modificação ou influência em virtude das novas tecnologias.

Com a migração dos ilícitos para o meio virtual, os meios de prova, que passaram a merecer especial atenção dadas as peculiaridades da tecnologia digital, são a prova documental, a prova pericial e também a busca e apreensão.

Quando falamos em ilícitos praticados pela Internet, necessariamente serão examinados registros, os quais são considerados documentos. E mesmo para os crimes em geral, como já pontuado, as evidências digitais se fazem presentes no dia a dia, pois os documentos assumiram a forma digitalizada.

Documento é *toda base materialmente disposta a concentrar e expressar um pensamento, uma ideia ou qualquer manifestação de vontade do ser humano, que sirva para expressar e provar um fato ou acontecimento juridicamente relevante. São documentos: escritos, fotos, fitas de vídeo e som, desenhos, esquemas, gravura, disquetes, CDs, DVDs, pen drives, e-mails, entre outros. Trata-se de uma visão moderna e evolutiva do tradicional conceito de documento – simples escrito em papel – tendo em vista o avanço da tecnologia.*[44]

A Lei nº 11.419/2006, que regula os processos eletrônicos, ao dispor sobre a informatização do processo judicial, prevê no seu artigo 11 que os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia de origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.

Essa disposição legal demonstra a assertiva de Nucci de que o conceito de documento não se restringe mais ao papel, tendo sido estendido aos registros digitais.

---

43 CINTRA, Antonio Carlos de Araujo. *Teoria Geral do Processo*. Antônio Carlos de Araújo Cintra, Ada Pellegrini Grinover, Cândido R. Dinamarco. Editora Revista dos Tribunais. 8ªedição, revista e ampliada. 1991.

44 NUCCI, Guilherme de Souza. *Provas no processo penal*. São Paulo: Editora Revista dos Tribunais, 2009.

As provas digitais possuem alto grau de volatilidade, sendo facilmente manipuláveis. Elas podem sofrer alteração pelo usuário ao tentar, este, apagar os rastros digitais do ilícito que cometeu. O próprio investigador pode, inadvertidamente, alterar as evidências digitais pela manipulação inadequada destas durante as etapas de aquisição e análise.

A partir dessa assertiva, a perícia pode ser necessária para comprovar a autenticidade do documento digital, que pode ser evidência de um ilícito eleitoral, praticado por meio dos sistemas informatizados ou Internet, ou que possui associado a si evidências com registro digital.

As provas digitais possuem determinadas características que devem ser observadas no seu tratamento em geral. A alta volatilidade já mencionada, que possibilita fácil alteração da prova, recomenda atenção e verificação da autenticidade por meio das técnicas periciais. Por isso, as provas que se encontram em poder dos provedores de aplicação devem ser objeto de preservação imediata, tão logo os investigadores dela tenham conhecimento, pois mesmo que obedecidos os prazos de retenção, este pode estar findando. Logo, a primeira coisa a se fazer é pedir a preservação da prova para que esteja íntegra quando for obtida a necessária ordem judicial para sua entrega.

Já quando são encontradas diretamente, sem a intermediação dos provedores, todo cuidado deve ser tomado para que a integridade e autenticidade sejam asseguradas. O fato de poderem ser duplicadas sem maiores problemas vem como uma vantagem para a coleta e análise das provas digitais, pois dessa forma, pode-se preservar a prova original, analisando-se a "cópia", não se correndo o risco de, na própria análise ocorrer algum tipo de adulteração acidental. A facilidade de duplicação também vem a ser característica relevante, na medida em que facilita aos peritos a coleta de grande quantidade de material a ser analisado. Em uma apreensão de grande quantidade de equipamentos ou em havendo equipamentos de dimensões muito grandes, não é necessário removê-los do local, bastando fazer o espelhamento do *hardware* para que se proceda à análise do conteúdo.

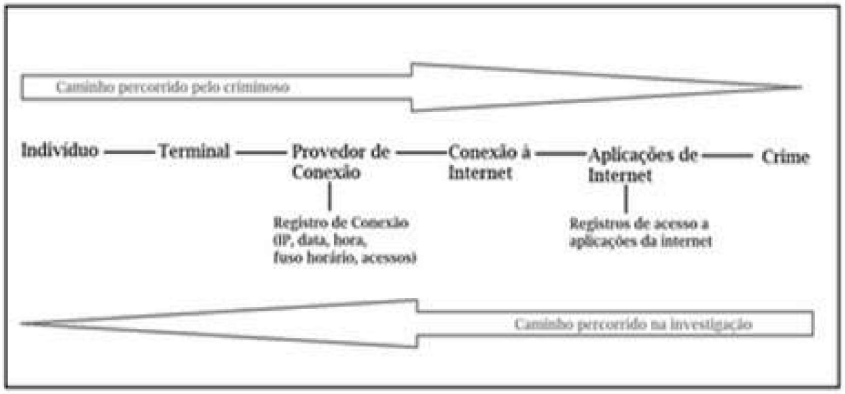
Outro fator que aponta vantagem aos investigadores do ilícito digital é a intangibilidade da evidência digital, tornando a sua destruição mais difícil. Devido à característica inerente dos equipamentos informáticos, é possível, por meio da prova pericial, recuperar os dados apagados, mesmo em datas posteriores ao evento delituoso.

A manipulação da prova digital deve ser adequada também visando a obtenção de metadados, pois estes a permeiam, sendo facilmente coletados na perícia e devendo ser fornecidos também pelos provedores de aplicações.

Devido à abundância de informações que é possível obter-se numa perícia de evidências digitais, o perito deve ser capaz de reduzir a quantidade de informações a fim de que estas possam ser organizadas para que seja exposto somente aquilo que é relevante para a investigação.

XII) Roteiro de Investigação

Para a investigação de uma conduta ilícita praticada pela internet é necessário atentar-se ao trajeto realizado pelo agente para a realização de tal conduta, pois o investigador realizará o caminho inverso para a identificação do usuário, conforme bem ilustram ALESSANDRO GONÇALVES BARRETO e BEATRIZ SILVEIRA BRASIL em seu Manual de Investigação Cibernética[45]:



Para o funcionamento da rede mundial de computadores, é necessária uma conexão à rede, que se realiza por meio de um *modem*, disponibilizado por um provedor de conexão. Esta conexão pode ser paga ou gratuita, mas implica em receber um número IP, isto é, um endereço de protocolo de Internet (*Internet Protocol)* exclusivo, pelo período da conexão, para acessar a infraestrutura de rede mantida pelas empresas de telecomunicações, como as operadoras de telefonia (Claro; Net; OI-Telemar; Tim; Vivo; etc). Esse IP pode ser utilizado pelo usuário para acessar serviços mantidos pelos provedores de aplicação de internet (site, Facebook; Instagram; WhatsApp; Google; Twitter; Microsoft; etc).

Importante: um mesmo número de IP pode ser utilizado por vários usuários durante determinado período, mas apenas por um único usuário em um dado dia e hora[46]. Por isso, é

45 v. BARRETO. Alessandro Gonçalves Barreto e Beatriz Silveira Brasil. Manual de Investigação Cibernética: À luz do Marco Civil da Internet. Brasport.

essencial que o IP venha acompanhado da data e horário exatos da conexão, incluindo o fuso horário, de forma a excluir outros usuários.

Em uma breve síntese, recebida uma denúncia de publicação de desinformação, com fins eleitorais, em alguma aplicação de Internet (*site*; mensageiro instantâneo; rede social; *email* etc), com uma simples consulta no endereço http://registro.br (para endereços nacionais) ou http://whois.icann.org (para endereços estrangeiros), é possível saber qual provedor de aplicação de internet é o responsável por aquele domínio pesquisado. O primeiro passo na investigação deve ser o pedido de preservação de dados dos registros de acesso e *logs* de *upload* (postagem) e de acesso à aplicação pelo usuário. Os grandes provedores costumam disponibilizar portais[47] para as autoridades fazerem esse pedido. Após o pedido de preservação, cabe o ajuizamento de medida cautelar de afastamento de sigilo telemático (Res. TSE 23.610/19, Art. 40 e MCI, Art. 22), para que o provedor de aplicação de internet indique, mediante ordem judicial, o IP, data e hora utilizados pelo usuário investigado na conexão àquela aplicação de internet. De posse dessas informações, outra consulta nos mesmos sítios[48] (com o número IP informado pelo provedor de aplicação), indicará qual empresa de telefonia é a responsável por alocar o IP pesquisado, à qual se deve dirigir o pedido de informação relativo à informação cadastral do cliente titular do serviço de conexão à internet. Essa informação será do endereço físico onde se deu a conexão de internet para a difusão/publicação do conteúdo investigado. A partir dos dados do titular do serviço, novas investigações devem ser feitas visando identificar o autor da postagem/ publicação.

A seguir, será detalhado o procedimento de investigação do usuário na Internet.

XII.1) Passos da Investigação: Do Que Se Trata a Notícia

Ao se tentar identificar o autor de um ilícito na Internet, o que pode ser requerido pela parte ao Juízo, em processo cível ou criminal, conforme prevê o art. 22 do MCI, reproduzido no art. 40 da Resolução TSE 23.610/2019, busca-se conhecer a materialidade reportada, a localização geográfica do conteúdo hospedado e finalmente o responsável pela sua publicação.

O primeiro passo para se iniciar uma investigação de um ilícito eleitoral, seja ele civil,

46 Exceção feita aos casos de uso do NAT-44, situação em que mais de um usuário está utilizando o mesmo IP no mesmo momento. Para esses casos, é preciso fazer um cruzamento de dados a partir de vários acessos com IPs diferentes para se identificar o usuário buscado.

47 https://facebook.com/records (Facebook e Instagram); https://WhatsApp.com/records (WhatsApp); https://ler-se.google.com (YouTube); https://legalrequests.twitter.com (Twitter).

48 http://registro.br (para endereços nacionais) ou http://whois.icann.org (para endereços estrangeiros).

como a prática de abuso de poder político, econômico ou dos meios de comunicação social, via internet (art.22 da LC 64/90); ou de natureza criminal, como a divulgação de uma notícia sabidamente falsa (Art. 326-A, do CE); contra a honra com fins eleitorais (Arts. 324 a 326 do CE), entre outros (art. 323 do CE e art. 35, da Resolução do TSE nº 23.610/2019, e Art.57-H, §§ 1º e 2º da Lei Eleitoral) é a identificação do que se trata a notícia, ou seja, qual ferramenta, das oferecidas pelos provedores de aplicações de Internet, foi utilizada e o provedor responsável por ela.

Tal informação será necessária tanto para a adoção de medidas quanto à preservação da prova quanto para a obtenção de informações acerca da autoria e materialidade do ilícito.

Os serviços mais comuns oferecidos pelos provedores de aplicações são a formação de redes sociais (ex: *Facebook, Instagram, Twitter,* etc); troca de mensagens instantâneas (WhatsApp, Telegram, Signal, etc); *email* (@gmail, hotmail, globo, terra, etc); páginas na word wide web - www (*sites*, *blogs, fotoblogs* etc); fóruns de discussão (ex.: Yahoo Groups); Voip (voz sobre IP); chat (salas de bate papo); hospedagem e compartilhamento de arquivos de fotos e vídeos (exs: eMule; Aresgalaxy; Gigatribe etc) e o e-commerce (ex.: Mercado Livre; Paypal etc).

Essa identificação dos responsáveis pelo serviço, se não for de fácil detecção ou mesmo para a obtenção de seus endereços, pode ser feita mediante consulta no serviço www.registro.br (para endereços nacionais) ou no http://whois.icann.org (para endereços no exterior).

XII.2) Passos da Investigação: Da Preservação das Provas (Autoria e Materialidade)

A prova digital é extremamente volátil, pois o usuário pode a retirar tão rápido quanto a publicou na Internet. Devemos garantir também a sua autenticidade, ou seja, de que a informação foi veiculada exatamente onde se está noticiando que ela foi e para assegurar sua integridade, que o manuseio dela não a alterará. Por isso, a necessidade de se obter o mais rápido possível a preservação dos dados de identificação do usuário e da própria publicação diretamente do provedor de aplicações.

Para a garantia da integralidade e da autenticidade da prova, duas medidas precisam ser imediatamente tomadas assim que se toma conhecimento da prática de ilícito: a) a coleta adequada da prova eletrônica; e b) a preservação dos dados referentes à prática de crime.

Assim que recebida a notícia da infração, sendo necessária a coleta da prova eletrônica (por ex.: *post* em rede social, *site*, *link* em mensageiro instantâneo, etc.), o promotor deve encaminhar a notícia à Divisão Especial de Inteligência Cibernética - DEIC, situada na sede do MP/RJ (faz parte da estrutura da Coordenação de Segurança Institucional - CSI), e que dá apoio aos promotores em questões relacionadas a investigações na Internet[49]. Ela deverá coletar adequadamente a prova utilizando ferramentas forenses que atestem que o material corresponde, exatamente, ao publicado, iniciando-se, a partir daí, a cadeia de custódia. Essa extração gerará um cálculo *hash*.

Ao mesmo tempo, deve ser requisitado ao provedor responsável (que mantém a rede social, que hospeda o *site*, etc.) a preservação dos dados cadastrais e dos *logs* (registros) de acesso referente ao ilícito, nos termos do art. 15, § 2º do MCI.

A notificação do provedor de aplicação de internet, responsável pelo serviço, para preservar os registros de acesso às aplicações, pode ser feita pelo membro do MP ou autoridade policial, sem ordem judicial, porque se está apenas solicitando que a empresa preserve os registros de acesso à aquela aplicação, que poderá, posteriormente, identificar o IP utilizado para postá-la e acessá-la, mediante o envio de uma ordem judicial.

Alguns provedores de aplicações mantêm canais específicos para pedidos de preservação e para envio de ordens judiciais através de endereços de *e-mail* destinados às equipes montadas para responder às autoridades ou através de portais na própria Internet, criados especialmente para responder às autoridades. Em tópicos próprios, serão informados os canais de acessos dos principais provedores de aplicação.

Para os provedores de aplicação, que prestam serviços no País e aqui mantêm

49 DEIC – javersa@mprj.mp.br, 21 99989-1661 (técnico pericial João Bernardo Aversa, diretor).

escritório, e que não possuem canal específico para encaminhamento de pedidos e ordens de Autoridades, basta enviar um ofício requerendo a preservação da página ou do perfil investigado.

No caso de provedores de aplicações, que prestam serviços no País e aqui não mantêm escritório, é possível utilizar a rede 24/7 da Polícia Federal (que atende tanto às autoridades federais como estaduais) para solicitar a preservação dos dados, através do *e-mail* cybercrime_brazil_24x7@dpf.gov.br.

É importante a correta identificação através do endereço na *web*, a **URL[50] ou ID[51]** do perfil, de um grupo; de um vídeo etc[52], a fim de que a preservação seja feita corretamente, tanto do conteúdo quanto dos dados cadastrais e dados associados a essa página ou perfil, os chamados metadados. Em tópico próprio, será informado como reconhecer a URL ou ID dos principais provedores de aplicação.

Os metadados são os dados sobre dados. São importantes para a investigação pois, se corretamente analisados e associados, podem trazer informações relevantes acerca da autoria do ilícito.

Metadados de uma imagem: dados de GPS de onde a imagem foi tirada; qual o tipo de máquina; data e hora.

Metadados de documento: data e hora da criação do documento e última modificação.

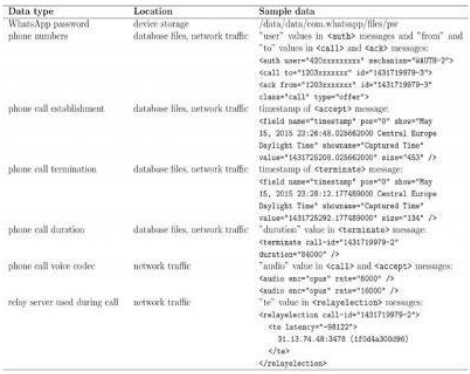
---

50 URL (Uniform Resource Locator) é a forma padronizada de representação de diferentes documentos, mídias e serviços de rede na Internet, que identifica de forma completa cada documento com um endereço único. Ex. http://www.uol.com.br/serviços.php

51 ID (Identificação ou user name), que é a identificação do usuário ou mais conhecido como Código de Usuário.

52 No caso de o denunciante usar o Facebook, veja o exemplo de uma URL de um PERFIL: https://www.facebook.com/barackobama : se o uso do Facebook foi pelo celular, precisa clicar no menu do aplicativo (3 pontinhos) e escolher a opção "copiar a URL". Às vezes, ao invés do nome, pode aparecer o ID, veja o exemplo de URL de um GRUPO com ID:
https://www.facebook.com/groups/982034701835686/
Exemplo de uma URL mostrando um vídeo no Facebook:
https://www.facebook.com/BBB18RedeGlobo2018/videos/199872690605072/
No Youtube, podemos identificar URLs de CANAL:
https://www.youtube.com/channel/UClu474HMt895mVxZdlIHXEA
Ou a URL de um vídeo específico:
https://www.youtube.com/whatch/v=2y-5hfZWADI

Metadados de comunicação: data e hora em que o usuário se comunicou com outro usuários e IPs utilizados; localização do usuário enquanto utiliza o serviço.



Data type	Location	Sample data
WhatsApp password	device storage	/data/data/com.whatsapp/files/pr
phone numbers	database files, network traffic	"user" values in <auth> messages and "from" and "to" values in <call> and <ack> messages: <auth user="420xxxxxxxx" mechanism="WAUTH-2"> <call to="1203xxxxxxx" id="1431719979-3"> <ack from="1203xxxxxxx" id="1431719979-3" class="call" type="offer">
phone call establishment	database files, network traffic	timestamp of <accept> message: <field name="timestamp" pos="0" show="May 15, 2015 23:26:48.025662000 Central Europe Daylight Time" showname="Captured Time" value="1431725208.025662000" size="453" />
phone call termination	database files, network traffic	timestamp of <terminate> message: <field name="timestamp" pos="0" show="May 15, 2015 23:28:12.177689000 Central Europe Daylight Time" showname="Captured Time" value="1431725292.177689000" size="134" />
phone call duration	database files, network traffic	"duration" value in <terminate> message: <terminate call-id="1431719979-2" duration="86000" />
phone call voice codec	network traffic	"audio" value in <call> and <accept> messages: <audio enc="opus" rate="8000" /> <audio enc="opus" rate="16000" />
relay server used during call	network traffic	"te" value in <relayelection> messages: <relayelection call-id="1431719979-2"> <te latency="-98122"> 31.13.74.48:3478 (1f04a300d96) </te> </relayelection>

Muitas vezes, o conteúdo investigado ainda está disponível na *web,* podendo ser coletado por um técnico em informática ou agente treinado para tal, que pode certificar a coleta da prova, devendo ser um agente público.

É muito importante que a cadeia de custódia da prova não seja quebrada, de forma que sua integridade se mantenha, garantindo sua autenticidade. De acordo com o Marco Civil da Internet, os provedores de aplicações, que prestam serviços no Brasil, devem reter os dados por seis meses. Porém, quando recebemos a notícia de um ilícito, não sabemos exatamente quanto tempo de retenção resta, de forma que sempre deve ser pedida a preservação dos dados e do conteúdo pretendido até que se obtenha a ordem judicial para sua obtenção.

XII.3) Passos da Investigação - Do Pedido de Retirada do Conteúdo

Como regra geral, o MCI apenas permite a retirada de conteúdo mediante ordem judicial, que analisará a natureza do conteúdo, reputando-o ilícito ou não, de forma que os provedores de aplicações de internet não serão responsabilizados pelo conteúdo gerado por terceiros, ao qual dão suporte, sem que haja ordem judicial específica determinando a remoção desse conteúdo, nos termos do art. 19 do MCI. Esse dispositivo foi reproduzido na Resolução TSE nº 23.610/2019, art. 38.

A Resolução TSE 23.610/2019, art. 7º,§ 1º, foi expressa em não admitir o exercício do poder de polícia da propaganda quando se tratar de controle de conteúdo postado na Internet. Nesses casos, será sempre necessária a provocação do juízo por parte de candidato, Partido ou MPE. Permanece o poder de polícia do juízo da propaganda nos casos em que a irregularidade não estiver no conteúdo, mas na forma ou meio da veiculação.

Entretanto, há três exceções que permitem a retirada de conteúdo imediatamente, sem ordem judicial, mediante contato direto com o provedor.

A primeira exceção diz respeito ao descumprimento de normas contidas nos termos de uso dos provedores de aplicação/conteúdo. Vários provedores, incluindo Facebook, Google e Twitter, possuem provimentos específicos, em seus termos de uso, para exclusão de conteúdo danoso, inclusive aquele com informações deturpadas.

A segunda exceção refere-se à prática de crime: quando a plataforma ou o serviço são utilizados para a prática de crime, é possível pedir diretamente ao provedor responsável a exclusão do conteúdo criminoso. Em regra, a utilização dos serviços para a prática de crime viola os termos de serviço dos provedores, o que permite a exclusão rápida.

A terceira e última exceção é legal e está prevista no art. 21 do MCI, que permite a exclusão de conteúdo de caráter sexual publicado sem a permissão do participante após notificação do interessado, sem a necessidade de ordem judicial.

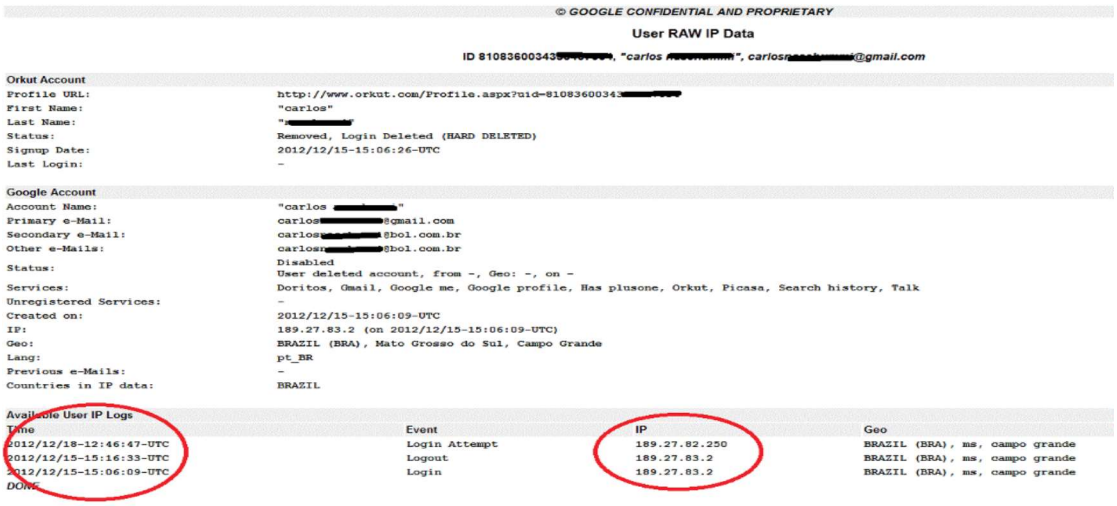
Importante: o pedido de exclusão de conteúdo, inclusive criminoso, deve ser sempre acompanhado de pedido de preservação dos dados referentes à página ou publicação, de modo que a prova não se perca. Assim, verificado conteúdo ilícito, o promotor deve pedir a preservação dos dados, como mencionado no item anterior, e depois, ou concomitantemente, a exclusão do conteúdo, mas jamais a exclusão antes de assegurada a preservação.

XII.4) Passos da Investigação - Do Pedido de Afastamento do Sigilo de Dados Telemáticos junto ao Provedor de Aplicações de Internet

Após o pedido de preservação e/ou de retirada de conteúdo nocivo, deve ser requerido judicialmente o afastamento de sigilo de dados telemáticos, nos casos criminais e nos casos cíveis, com base no artigo 10, §§ 1º e 2º c/c art. 22, ambos do MCI (Res. TSE 23.610/2019, arts. 39 e 40).

O primeiro pedido de quebra deve ser direcionado ao provedor de aplicação à Internet, que mantém o serviço/aplicação onde foi publicado o conteúdo ilícito. Ele deve ser instruído com a prova colhida na forma mencionada nos itens anteriores, bem como a indicação clara da página/postagem investigada, com a indicação do endereço URL e /ou ID.

O pedido de afastamento deve requerer que o Juízo respectivo requisite do provedor de aplicação à Internet responsável pelo serviço as informações de IP de criação, data e hora dos registros de postagem (*uploads*) e acessos, ao perfil/página. Também deve ser requerido que o provedor encaminhe outras informações relacionadas, como *e-mail*, nome cadastrado, *nickname* (apelido), contatos de pagamento (por ex.: número de cartão de crédito). Exemplo de uma resposta:



© GOOGLE CONFIDENTIAL AND PROPRIETARY

User RAW IP Data

ID 810836003435[redacted], "carlos [redacted]", carlos[redacted]@gmail.com

Orkut Account

Profile URL:	http://www.orkut.com/Profile.aspx?uid=810836003[redacted]
First Name:	"carlos"
Last Name:	"[redacted]"
Status:	Removed, Login Deleted (HARD DELETED)
Signup Date:	2012/12/15-15:06:26-UTC
Last Login:	-

Google Account

Account Name:	"carlos [redacted]"
Primary e-Mail:	carlos[redacted]@gmail.com
Secondary e-Mail:	carlos[redacted]@bol.com.br
Other e-Mails:	carlos[redacted]@bol.com.br
Status:	Disabled User deleted account, from -, Geo: -, on -
Services:	Doritos, Gmail, Google me, Google profile, Has plusone, Orkut, Picasa, Search history, Talk
Unregistered Services:	-
Created on:	2012/12/15-15:06:09-UTC
IP:	189.27.83.2 (on 2012/12/15-15:06:09-UTC)
Geo:	BRAZIL (BRA), Mato Grosso do Sul, Campo Grande
Lang:	pt_BR
Previous e-Mails:	-
Countries in IP data:	BRAZIL

Available User IP Logs

Time	Event	IP	Geo
2012/12/18-12:46:47-UTC	Login Attempt	189.27.82.250	BRAZIL (BRA), ms, campo grande
2012/12/15-15:16:33-UTC	Logout	189.27.83.2	BRAZIL (BRA), ms, campo grande
2012/12/15-15:06:09-UTC	Login	189.27.83.2	BRAZIL (BRA), ms, campo grande

DONE

Em tópico próprio, constam modelos de medida cautelar de quebra de sigilo telemáticos, bem como os endereços dos principais provedores.

XII.5) Passos da Investigação – Do Pedido de Afastamento do Sigilo de Dados Telemáticos junto ao Provedor de Conexão à Internet

Com as informações recebidas do provedor de aplicações de internet, conforme o explanado no item anterior, incluindo o Internet Protocol – IP utilizado e a data e hora de utilização, será possível identificar o provedor de conexão, que alocou aquele IP, e requisitar a ele as informações referentes ao usuário que se conectou na internet através desse IP na data e hora indicados (art. 10, § 3o. do MCI).

A identificação do provedor de conexão (as operadoras de telefonia ou telecomunicações, que prestam serviços disponibilizando aquele endereço de IP específico) é feita a partir de uma consulta no *site* http://registro.br ou o https//whois.icann.org (informa os endereços de IPs no exterior).

A requisição, por se tratar de meros dados cadastrais, pode ser feita diretamente ao provedor de conexão identificado, de acordo com o art. 10, § 3º, do MCI. Entretanto, ainda há questionamentos sobre a necessidade ou não de intervenção judicial, sendo conveniente que o pedido seja feito ao Juízo, de modo a afastar qualquer futura alegação de nulidade. Em tópicos próprios, constam modelos de ofício com a requisição de dados cadastrais aos provedores de conexão, bem como os endereços dos principais provedores.

O endereço de IP utilizado identifica o dispositivo informático, seja ele um terminal de computador, celular, *tablet*, etc. Não significa necessariamente que o titular dos dados cadastrais, cliente daquela operadora, é o autor do fato, que foi o usuário que se está investigando. Esse cliente identificado pode ter emprestado seu sinal de *wifi* para um amigo, ou mesmo partilhar o mesmo sinal com vizinhos (fato comum em comunidades), ou ser utilizado por qualquer outra pessoa que com ele resida ou visite. Por isso, serão necessárias outras diligências para a confirmação da autoria.

XII.6) Passos da Investigação – Medida Cautelar de Busca e Apreensão

Com a identificação do endereço de onde partiram as imagens ou mensagens investigadas, a providência seguinte, no caso de investigação criminal, AIJE, AIME e representação por conduta vedada, é a busca e apreensão no local para confirmação da materialidade e individualização da autoria. A busca, autorizada judicialmente, permitirá apreender vestígios relacionados à prática do delito, incluindo eventual material e

equipamentos empregados, que deverão ser submetidos a perícia.

Não há legislação específica para quando essa medida se destinar à apuração de um ilícito praticado pela Internet, por isso são utilizadas as normas referentes à busca e apreensão previstas no Código de Processo Penal (art. 240, § 1º, alínea "e" e "h") e no Código de Processo Civil (artigos 842 e 843).

Nada impede que a cautelar seja requerida no âmbito de um procedimento investigatório de natureza eleitoral, aplicando-se subsidiariamente as legislações processuais civil e penal.

Saliente-se que o mandado de busca e apreensão deve ser específico, elencando um rol amplo de possibilidades para a apreensão, a fim de se evitar dúvidas que possam vir a gerar nulidades, incluindo diversos tipos de equipamentos (computadores, celulares, *tablets*, câmeras fotográficas, mídias de armazenamento, etc.).

Importante: Em relação aos aparelhos celulares, que são hoje muito mais que meros telefones, mas sim computadores pessoais, que armazenam milhares de dados, a jurisprudência mudou. Em 2007, decisão do STF dizia bastar um mandado genérico para se ter acesso a todo o conteúdo de um celular apreendido. Em 2016, o STJ, no HC 51.531, decidiu ser necessária autorização específica para que os agentes de investigação tivessem acesso ao conteúdo do aparelho celular apreendido em uma prisão em flagrante. Recentemente, foi reconhecida a Repercussão Geral pelo Supremo Tribunal Federal, ao Agravo em Recurso Extraordinário ARE nº 1.042.075, em que se discute exatamente essa questão: de que para acesso ao aparelho celular apreendido, para conhecimento do registro das chamadas e da agenda de telefones, bem como das demais informações, é necessária prévia autorização judicial. Nesse quadro, de forma a evitar futura alegação de nulidade, é conveniente pedir autorização judicial para acesso de cada um dos equipamentos apreendidos, inclusive celulares e *tablets*.

Armazenamento na nuvem (*cloud computing*): armazenamento nas nuvens permite que arquivos sejam guardados em servidores remotos, instalados em local diverso de onde o equipamento deve ser apreendido. Inúmeros provedores oferecem serviços que permitem armazenamento de arquivos nas nuvens (Google, Microsoft, Apple, etc.). O armazenamento pode ocorrer em serviços destinados a isto, como Google Drive, ou em outros serviços que oferecem espaço, como *e-mails*.

Normalmente, para acessar esses arquivos é necessário fornecer uma senha. Essa pode ser fornecida espontaneamente pelo investigado para acesso aos arquivos remotos, e nesse caso, o perito que estiver acompanhando o cumprimento da diligência de busca e apreensão,

pode acessar e coletar esses arquivos e toda evidência digital relacionada a eles, de forma sincronizada.

Caso o dispositivo esteja desconectado com a nuvem, a perícia terá que obter a senha, utilizando programas de descriptografia. Muitos arquivos na nuvem não são criptografados.

Uma alternativa para a obtenção de arquivos mantidos na nuvem caso não haja colaboração do investigado é a requisição direta ao provedor responsável pelo serviço. O pedido, neste caso, demanda autorização judicial e poderá englobar todos os arquivos e informações mantidos pelo provedor, desde que detalhados na autorização.

Após a busca e apreensão, feita pela autoridade policial ou ministerial, visando identificar a autoria, caso residam mais de uma pessoa no local onde foi apreendido o dispositivo informático ou caso o sinal de Internet seja compartilhado com terceiros. Essa apuração será mais simples dependendo dos elementos colhidos durante a busca, como a identificação do dono do celular de onde partiram as publicações.

No entanto, quando a investigação for cível, identificado o usuário que divulgou a notícia, pelo provedor de aplicações de internet, que informou o IP, e pelo provedor de conexão, que informou os dados cadastrais do usuário, que utilizou aquele IP, muitas vezes, não há necessidade de busca e apreensão daquele arquivo, que já é público. Basta a identificação do usuário do IP, que se conectou à Internet, por determinado dispositivo e fez a referida publicação. Mas caso haja negativa da autoria delitiva, somente a perícia no dispositivo informático apreendido poderá confirmá-la.

Os grandes provedores de aplicações de internet, que prestam serviços no País, como *Facebook*[53] e *Twitter*[54] dizem que deletam perfis falsos, fazem campanhas sobre *fake news* e colaboram com as autoridades. É necessário, outrossim, o constante desenvolvimento e aperfeiçoamento de ferramentas já existentes na própria aplicação, que identifiquem os robôs (*bots*), muito utilizados para propagar desinformação em seus serviços, e a identificação de usuários que descumprim os próprios Termos de Serviços das plataformas.

XII.7) Desinformação veiculada por *sites*

Temos visto inúmeras páginas na *web* – *sites* – falsos, se fazendo passar pela página de alguém, algum estabelecimento ou instituição.

Os mensageiros eletrônicos e as demais redes sociais propagam *links* que levam a

53 http://agenciabrasil.ebc.com.br/geral/noticias/2017-12/0-que-diz-o-facebook-em-relacao-fake-news

54 Reunião realizada na sede da PR/SP, em 25.04.2018, com representantes do Twitter, Vice-PGE e membros do GACC.

essas páginas através de postagens também falsas.

O ideal é que tais postagens sejam retiradas das redes sociais, porém, devido à dimensão da Internet e à rápida difusão dessas mensagens, nem sempre isso é possível, sendo necessário retirar/desabilitar o conteúdo do *site* para que não fique mais disponível a quem acessá-lo.

Assim que recebida a notícia da infração, sendo necessária a coleta da prova eletrônica, isto é, a prova da existência da página, o promotor deve encaminhar a notícia à Divisão Especial de Inteligência Cibernética- DEIC[55], que deverá coletar adequadamente a prova utilizando ferramentas forenses que atestem que o material corresponde, exatamente, ao publicado, iniciando-se, a partir daí, a cadeia de custódia. Essa extração gerará um cálculo hash. A técnica para fazer essa extração de maneira adequada, deve ser realizada pelo DEIC.

Além da preservação da prova, a próxima providência será a identificação de onde o *site* está hospedado. Em geral os criminosos se utilizam de um serviço de hospedagem, como GoDaddy, UOL ou worldpress.

O serviço de hospedagem, em que o *site* malicioso está albergado, em tese, tem como informar os dados da pessoa que criou o *site* malicioso, o IP de criação e os *logs* de acesso ao *site*. O problema é que, em geral, os criminosos se utilizam também de um serviço de anonimização, isto é, se valem dos serviços de uma empresa de privacidade *on-line* para que ela registre o *site* na empresa de hospedagem no lugar do real proprietário do domínio, como forma de dificultar a sua identificação. Essa empresa, que registrou o *site* como seu, é que possui a informação do real proprietário (dados cadastrais, inclusive financeiros).

Para identificar o provedor de hospedagem e eventual provedor de anonimização, devem ser consultados os serviços https://www.registro.br/ (para endereços nacionais) e no http://whois.icann.org (para endereços no exterior), nos termos do item XII.2 acima.

Vejamos um exemplo de um *site* fraudulento, que simulava um endereço oficial do Governo Federal para angariar dados e inocular códigos maliciosos, antes acessível pelo endereço eletrônico https://cadastroauxilio.online/Beneficio/?AuxilioEmergencial:

55 DEIC – Divisão Especial de Inteligência Cibernética –javersa@mprj.mp.br, tel 21 99989-1661 (Diretor João Bernardo Aversa – técnico pericial), que integra a estrutura da Coordenação de Segurança Institucional (coordenadora Elisa Fraga, tel 21 99989-1661)

Após pesquisa realizada em http://whois.icann.org (ou https://lookup.icann.org/lookup), foi possível constatar que a empresa, que hospeda o *site* malicioso, está oculta e somente pode ser identificada se entrarmos em contato com a empresa *Cloudflare*, que consta como *name server*, a Hostinger aparece como o Registrador e a Privacy Protect LLC, que oferece serviços de privacidade, está no lugar do Registrante (ver quadro abaixo). A empresa *Cloudflare* é a que tem a informação acerca da hospedagem do *site* malicioso e a quem deve ser questionado quem hospeda o *site*. Uma vez sabendo quem é o provedor de hospedagem, a ele deve ser direcionado o pedido de preservação de registros de criação do *site* e *logs* de acesso (IPs, data e hora) e o pedido de remoção do *site* malicioso da Internet. A empresa Privacy Protect é a que aparece como responsável pelo *site* malicioso, a Registrante deve ser interpelada para preservar os dados do real usuário (dados cadastrais, inclusive financeiros) para futuro encaminhamento, após obtenção de ordem judicial para este fim. Outra providência pode ser contatar a Hostinger, que no caso é a Registradora, para que seja retirado o domínio malicioso do ar.

Domain Information

Domain:	cadastro-auxilio.online
Registrar:	Hostinger, UAB
Registered On:	2020-03-31
Expires On:	2021-03-31
Updated On:	2020-03-31
Status:	serverTransferProhibited clientTransferProhibited addPeriod
Name Servers:	ophelia.ns.cloudflare.com chad.ns.cloudflare.com

Registrant Contact

Organization:	Privacy Protect, LLC (PrivacyProtect.org)
State:	MA

Caso as empresas responsáveis pela hospedagem e anonimização sejam brasileiras ou tenham filial no Brasil, os pedidos de preservação devem ser endereçados a elas diretamente nos termos do item XII.2 acima.

Relembre-se que para a empresa responsável pela hospedagem deve também ser direcionado o pedido de remoção do *site* malicioso, frente a possibilidade de que o provedor verifique violação dos seus termos de serviço e retire espontaneamente o *site* da Internet.

Posteriormente, o Promotor deve ajuizar a medida cautelar de quebra de sigilo telemático, com o pedido para a ordem judicial de remoção do *site*.

Caso a empresa a ser demandada não tenha vínculo com o Brasil, duas medidas podem ser tomadas simultaneamente. Essas empresas costumam possuir uma aba ou *email* para reportar abusos, o que pode ser feito diretamente a fim de avisar a empresa sobre o conteúdo ilícito, já pedindo preservação dos dados e a remoção do *site* ilícito, reforçando sobre a necessidade de não haver a notificação do responsável pelo *site* a fim de não prejudicar a investigação.

Concomitantemente, deve-se pedir o auxílio da Polícia Federal através do *e-mail* cybercrime_brazil_24x7@dpf.gov.br, também pedindo preservação dos dados e a remoção do *site* malicioso.

Após, deve-se realizar o ajuizamento de pedido judicial de quebra de sigilo telemático do *site* a fim de instruir o pedido de cooperação internacional para obtenção formal das informações relativas ao *site* investigado.

Relembre-se que para todas as medidas extra e judiciais o *site* deve ser identificado com o seu endereço eletrônico (URL) completo.

XII.8) Desinformação veiculada pelo Facebook e Instagram

Recebida representação de que houve a veiculação, no Facebook ou Instagram, de mensagem com conteúdo ilícito, a primeira providência é adoção de medidas de preservação dos registros relacionados a esta mensagem e do usuário que a emitiu, como mencionado no item XII.2.

Para tal finalidade, é importante que se identifique a conta do perfil que se pretende investigar (v. https://www.facebook.com/safety/groups/law/guidelines/).

As contas do Facebook podem ser identificadas pelo: a) URLs das contas com o número de identificação de usuário (http://www.facebook.com/profile.php?

id=1000000XXXXXXXX) ou com o nome de usuário (http://www.facebook.com/nomedeusuario) do perfil do Facebook, b) endereço de *e-mail* e c) o número de telefone (+55, DDD, número).

Para a localização do endereço eletrônico do perfil investigado (URL), no computador, ao acessar a página do perfil, a URL é exibida na barra de endereços do navegador.

No celular, o acesso à URL do perfil é obtido após o clique no menu e a seleção de "copiar link". Após clicar em "copiar link", deve-se "colar" essa informação em qualquer arquivo de texto.

Obtidas as informações em relação a conta investigada, acesse o Sistema do Facebook de Solicitação On-Line para Autoridades, localizado em https://www.facebook.com/records, e siga as instruções para a preservação da conta.

Ao mesmo tempo em que se busca a preservação dos dados junto ao Facebook, é necessário a colheita adequada da prova, com todos os cuidados forenses para que seja mantida íntegra e preservada, dando-se início à cadeia de custódia. Para tanto, as informações necessárias para acesso à publicação devem ser encaminhadas de imediato ao setor especializado na sede do MP (DEIC), para extração do cálculo *hash*, nos termos mencionados no item XII.2. Na DEIC, o setor de TI terá condições técnicas de fazer essa extração de maneira adequada.

Realizado o pedido de preservação e colheita da prova, caso se considere necessária a retirada do conteúdo da rede social, é importante que se obtenha a URL específica da postagem que se pretende remover. A retirada de conteúdo, como exposto acima, precisa limitar-se especificamente à URL infratora, sob pena de ser retirado também conteúdo lícito (quando, por exemplo, se solicita a retirada de um perfil inteiro, que contém conteúdo lícito e ilícito).

No Facebook, cada perfil, página, evento ou grupo possui uma URL própria e genérica que, por sua vez, é mais ampla e diferente das URLs mais específicas das publicações ou comentários neles existentes. Em uma página, grupo ou evento, determinada publicação poderá ter sido feita por usuários diferentes que tenham poderes sobre aquele ambiente, motivo pelo qual é importante que se identifique a URL específica da publicação tida como ilícita.[56]

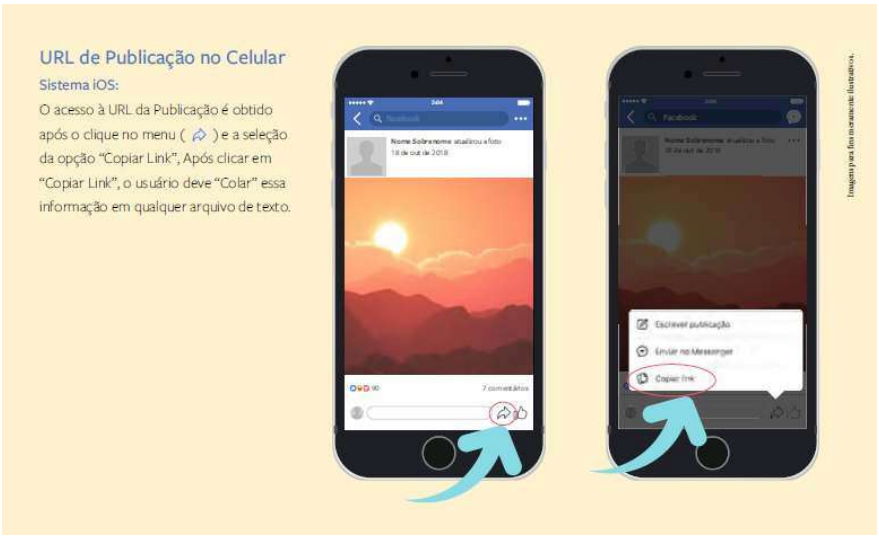
No computador, para identificação da URL específica de uma publicação ou comentário, clique na respectiva data ou hora de disponibilização, que a URL aparecerá na barra de endereços do navegador, conforme imagem a seguir[57]

No celular, o acesso à URL da publicação é obtido após o clique no menu e a seleção da opção copiar link. Após clicar em "copiar link", deve-se "colar" essa informação em qualquer arquivo de texto[58]

56 v. www.tre-rj.jus.br/site/eleicoes/2018/arquivos/cartilha_identificacao_usuarios.pdf

57 Imagem obtida em www.tre-rj.jus.br/site/eleicoes/2018/arquivos/cartilha_localizacao_especificacao_conteudo.pdf

58 Imagem obtida em www.tre-rj.jus.br/site/eleicoes/2018/arquivos/cartilha_localizacao_especificacao_conteudo.pdf



Para melhor detalhamento de obtenção de URLs, acesse as seguintes cartilhas: www.trerj.jus.br/site/eleicoes/2018/arquivos/cartilha_localizacao_especificacao_conteudo.pdf e www.tre-rj.jus.br/site/eleicoes/2018/arquivos/cartilha_identificacao_usuarios.pdf.

A retirada de conteúdo, como mencionado no item XII.3, somente pode ser feita sem ordem judicial em determinadas hipóteses. Nesses casos, depois de identificada a URL específica, como mencionado acima, pode ser feito o pedido de retirada diretamente ao Facebook, por meio de *e-mail* enviado ao endereço records@facebook.com, com o *link* do conteúdo a ser retirado.

Após a preservação da prova, e a retirada do conteúdo, caso seja necessário, o próximo passo é o ajuizamento de medida cautelar de quebra de sigilo telemático para obtenção dos registros de acesso, cujo modelo encontra-se em tópico próprio (item XII.5), seguindo-se os demais passos expostos nos itens XII.6 e XII.7.

Importante: o Facebook notifica os usuários quanto a pedidos de informação referentes a seus dados. Por isso, caso o sigilo seja indispensável para a investigação, é necessário indicar à empresa que o pedido não poderá ser informado ao usuário.

Reitere-se que o meio de comunicação para entrega de ofícios ao Facebook é a plataforma https://www.facebook.com/records.

Por fim, nos ofícios, deve constar o endereço da matriz do Facebook/Instagram:

Facebook, Inc., 1601 Willow Road, Menlo Park, CA 94025, California, United States
A/C do Facebook/ Instagram Brasil
Rua Leopoldo Couto de Magalhães Junior, 700, 5º andar
Bairro Itaim Bibi
São Paulo -SP
CEP 04542-000

XII.9) Desinformação Veiculadas pelo WhatsApp

Na hipótese de veiculação de mensagens com conteúdo ilícito pelo aplicativo WhatsApp, o pedido de preservação de dados deve ser realizado pelo sistema de Solicitação On-Line para Autoridades, localizado no https://www.whatsapp.com/records, bastando seguir as instruções.

Para esta finalidade, é necessário que se tenha a conta a ser investigada que será identificada pelo número do telefone do usuário (+55-DDD-número).

Sem prejuízo, deve ser feita a coleta da prova nos termos indicados no item XII.2, com a remessa das informações ao setor de TI (DEIC-CSI)

Importante: as mensagens de WhatsApp podem conter dois tipos diferentes de meios de propagação. O primeiro é envio do arquivo, ou mensagem, no próprio sistema do aplicativo. Nesses casos, deve ser seguido o roteiro indicado abaixo neste item para colheita da mensagem e investigação da origem. O segundo é o envio de *link* que remete a outro *site* na Internet, que é o que efetivamente contém o conteúdo ilícito. Neste caso, não basta ser excluída a mensagem, pois o *site* continuará funcionado, devendo ser seguido o roteiro indicado no item XII.7.

Após o pedido de preservação e a coleta da prova, o próximo passo é o ajuizamento da medida cautelar de quebra de sigilo de dados do provedor de aplicação (item XII.4), pela qual é possível solicitar diversas informações dos usuários, como abaixo especificado:

- dados de perfil (foto, nome, número de telefone, sistema operacional, data da criação da conta, versão do WhatsApp instalado, e endereço de *e-mail*, se fornecido) - esses dados também podem ser obtidos sem ordem judicial;
- informação dos grupos onde o investigado participa, incluindo os participantes;
- grupos onde o usuário é administrador;
- última conexão com data, hora e IP, se disponível;
- indicação de *e-mail* que foi utilizado para *backup* de mídia e mensagens, se

disponível;

- histórico de mudança de números; e
- agenda de contatos.

Importante: as comunicações realizadas através do WhatsApp utilizam criptografia ponta-a-ponta. Isso significa que a empresa não possui as mensagens e nem é possível interceptá-las. É possível, porém, ajuizar medida de interceptação telemática visando obter os dados das comunicações, mas não o conteúdo. Nesses casos, é possível solicitar o envio de:

- extratos de mensagens, consistente nas informações de remetente, destinatário, data e hora da mensagem;
- tipo da mensagem; e
- IP da conta alvo, se disponível.

Pode ser solicitado que tais informações sejam repassadas a cada 24 horas, contadas da data de implementação da medida até os 15 (quinze) dias seguintes a esta.

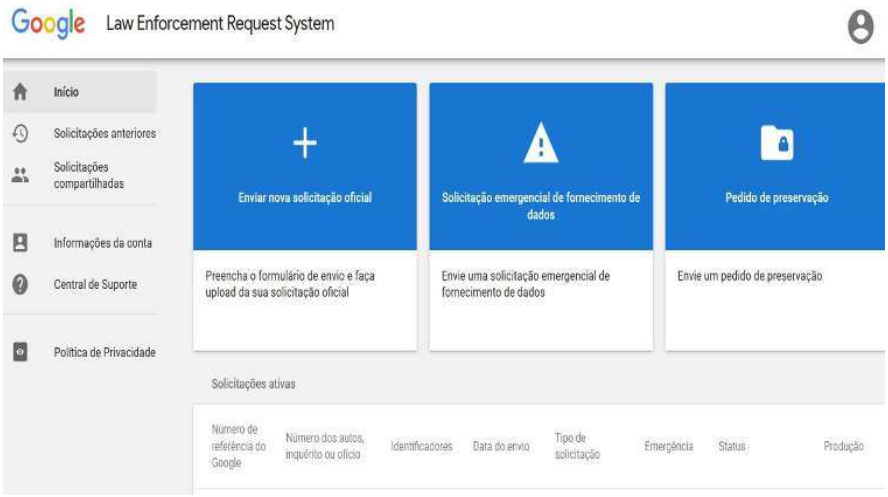
Repise-se que os ofícios devem ser encaminhados pelo sistema de Solicitação On-Line para Autoridades, localizado no https://www.whatsapp.com/records:

Por fim, nos ofícios, deve constar o endereço do Facebook, como segue:

Facebook, Inc., 1601 Willow Road, Menlo Park, CA 94025, California, United States
A/C do Facebook/Instagram Brasil
WhatsApp Inc.
Rua Leopoldo Couto de Magalhães Junior, 700, 5º andar,
Bairro Itaim Bibi, São Paulo-SP
CEP 04542-000

XII.10) Desinformação Veiculada pelo Youtube

Na hipótese de veiculação de conteúdo ilícito pelo Youtube, o pedido de preservação de dados deve ser realizado pelo sistema de Law Enforcement Request System da Google, acessível pela URL http://lers.google.com, na qual será necessária a criação de conta.



A preservação de dados ou encaminhamento de ofícios também poderá ser realizada pelos *e-mails*: lis-latam@google.com e juridicobrasil@google.com.

Como nos casos anteriores, concomitantemente ao pedido de preservação, é necessário coletar a prova por meio de ferramentas forenses, conforme descrito no item XII.2, encaminhando-se ao setor de TI da sede do MP, no caso, o citado DEIC-CSI.

Também é possível solicitar a retirada do conteúdo nocivo, nos termos descritos no item XII.3. O *link* para remover conteúdo do YouTube caso viole seus Termos de Serviço: https://www.youtube.com/reportingtool/legal.

Após, deve ser providenciado o ajuizamento de medida cautelar de quebra de sigilo telemático, nos termos descritos no item XII.4, para obtenção das seguintes informações, entre outras:

- *logs* de acesso (contendo IP, data, hora e fuso horário GMT) de criação do canal e dos acessos em período a ser indicado;

- endereços eletrônicos e outros dados eventualmente armazenados do criador da página; e

- dados da conta Google, incluindo informações de localização, dados armazenados do Google Maps, histórico de pesquisa do Google, imagens armazenadas no Google Photos, dados armazenados no Google Drive, etc.

Recomenda-se que o ofício seja enviado pelo Sistema de Law Enforcement Request System da Google, acessível pela URL http://lers.google.com e tenha o seguinte endereçamento:

Google Brasil Internet Ltda.
Avenida Brigadeiro Faria Lima, 3477, 18º andar
São Paulo - SP
CEP 04538-133

XII.11) Desinformação veiculadas pelo Twitter

Na hipótese de veiculação de conteúdo ilícito pelo Twitter, o pedido de preservação de dados deve ser realizado pelo sistema on-line https://legalrequests.twitter.com.

O pedido de preservação deve conter a identificação do perfil infringente, com as seguintes informações (v. https://help.twitter.com/pt/rules-and-policies/twitter-law-enforcement-support#6): o nome do usuário e o URL do perfil do Twitter envolvido (por exemplo, https://twitter.com/twittersafety (@twittersafety); e/ou o número de identificação do usuário ou UID exclusivo e público da conta no Twitter ou um nome de usuário e URL do Periscope (por exemplo, @twittersafety e https://periscope.tv/twittersafety). Para localizar um UID do Twitter ou o nome de usuário do Periscope, consulte https://help.twitter.com/pt/rules-and-policies/twitter-law-enforcement-support#5.7.

Realizado o pedido de preservação, a notícia de fato deve ser encaminhada ao setor de TI do MP (DEIC-CSI) para este realizar a preservação das informações trazidas na notícia de fato, nos termos descritos no item XII.2.

Caso seja necessária a retirada do conteúdo, nos termos do descrito no item XII.3, seguir as orientações publicadas em https://help.twitter.com/pt/rules-and-policies/twitter-law-enforcement-support#16.5.

Após a preservação, e a retirada, se necessária, o próximo passo é o ajuizamento de Medida Cautelar de Afastamento de Sigilo Telemático, nos termos descritos no item XII.4,

em que podem ser pleiteadas diversas informações sobre o usuário, tais como:

- *Logs* de acesso (IP, data, horário e fuso horário) do período indicado (referente à publicação da mensagem);
- nome, sobrenome, senha, *email* e nome de usuário;
- localização, foto da conta e do fundo;
- número de celular para recebimento de SMS e catálogo de endereços;
- *tweets*, as contas seguidas, *tweets* favoritos;
- coordenadas exatas da localização dos *tweets*;
- endereços de IP, data/hora/fuso, navegador utilizado, domínio referentes, páginas visitadas, operadora do dispositivo móvel;
- dispositivo móvel, Ids de aplicativos e termos de busca; e
- links visitados e quantidade de vezes que foi clicado.

Importante constar no requerimento que o ofício pode ser enviado pelo *site* de Envios de Solicitação Legal (http://legalrequests.twitter.com) e possuir o seguinte endereçamento:

Twitter, Inc.
c/o Trust and Safety
795 Folsom Street, Suite 600
San Francisco, CA 94107
Twitter Brasil Rede de Informação Ltda.
Rua Professor Atílio Innocenti, 642, 9º Andar
Vila Nova Conceição, São Paulo-São Paulo
CEP 04538-001

Importante: o Twitter notifica usuários sobre as solicitações de informação da conta, motivo pelo qual é importante que, em qualquer pedido, inclusive o de preservação, conste o requerimento para que o usuário não seja notificado, com a indicação de que a ciência será prejudicial à investigação. Deve ser apontado, também e na medida do possível, o prazo em que essa comunicação não poderá ser feita.

Por fim, cabe ressaltar que as operadoras do Twitter atribuem o "selo azul de verificação" às contas de interesse público, ou seja, as operadoras do Twitter analisam os dados fornecidos pelos titulares e confirmam que estes são autênticos e que efetivamente pertencem à pessoa ou à marca que representam (v. https://help.twitter.com/pt/managing-your-account/twitter-verified-accounts). Tal informação pode ajudar a verificar se o *tweet* investigado partiu realmente do titular da conta.


SECOMVC
Seguir
SecomVc
@secomvc
Bem-vindos ao SecomVc, canal da Secretaria Especial de Comunicação Social da Presidência da República. Aqui vamos manter diálogo direto e combater as fake news.
gov.br
Ingressou em agosto de 2019
seguindo 125
85,9 mil seguidores
Tweets
Tweets e respostas
Mídia
Curtidas

XIII) MODELO DE PEÇA DE MEDIDA CAUTELAR DE QUEBRA DE SIGILO TELEMÁTICO PARA SERVIDOR DE HOSPEDAGEM E PRIVACIDADE DE SITES ILÍCITOS

EXCELENTÍSSIMO SR. JUIZ ELEITORAL DA ___Nº ZONA ELEITORAL ...

SIGILOSO

Procedimento nº:

O MINISTÉRIO PÚBLICO ELEITORAL, pelo (a) Promotor (a) de Justiça Eleitoral, que ao fim assina, com fulcro em suas atribuições constitucionais e legais, vem à presença de Vossa Excelência requerer, com fulcro no artigo 5º, inciso XII, da Constituição Federal e no artigo 10, § 1º, da Lei 12.965/14 (Res TSE 23.610/2019, art. 39), MEDIDA CAUTELAR DE QUEBRA DE DADOS TELEMÁTICOS, pelos motivos de fato e direito abaixo expostos:

I – DOS FATOS

Dos fatos investigados

O procedimento, em epígrafe, foi instaurado para apurar a possível prática do ilícito tipificado no artigo XX da .

Conforme consta na notícia, o *site* [indicar URL] simula ser um *site* oficial do Governo Estadual, com o fim de angariar dados dos usuários e inocular códigos maliciosos, conforme se nota pelas imagens abaixo:

[Incluir imagens da captura de tela do site]

Frente a tal informação, solicitou-se a preservação dos registros referentes ao mencionado *site*, tanto para o provedor de hospedagem como para o serviço de anonimização (v. fls.), bem como solicitou-se ao setor de Tecnologia e Informação do MP/RJ, realizasse a colheita da prova, com extração do cálculo *hash*, o que foi cumprido, conforme fl. X.

Dessa forma, revela-se imperiosa, para a elucidação do delito penal sob investigação, a quebra de sigilo de dados telemáticos do responsável pelo site [indicar URL], de modo a viabilizar sua identificação e reunir elementos probatórios acerca da prática criminosa investigada.

1.2) Das Diferenças entre Serviço de Hospedagem e de Anonimização

Para melhor entendimento do pleito ministerial, faz-se necessário o conhecimento acerca da diferença entre serviço de hospedagem e de anonimização de *sites*.

Os *sites* são disponibilizados na internet, através do servido de hospedagem. Em geral os criminosos se utilizam de um serviço de hospedagem, como GoDaddy, UOL ou worldpress.

Assim, o serviço de hospedagem em que o *site* está albergado, em tese, tem como informar os dados da pessoa que criou o *site*, o IP de criação e os *logs* de acesso ao *site*. O problema é que, em geral, os criminosos se utilizam também de um serviço de anonimização, isto é, se valem dos serviços de uma empresa de privacidade *on-line* para que ela registre o *site* na empresa de hospedagem no lugar do real proprietário do domínio, como

forma de dificultar a sua identificação. Essa empresa que registrou o *site* como seu é que possui a informação do real proprietário (dados cadastrais, inclusive financeiros).

Para identificar o provedor de hospedagem e eventual provedor de anonimização, devem ser consultados os serviços https://www.registro.br/ (para endereços nacionais) e no http://whois.icann.org (para endereços no exterior).

Após pesquisa realizada em http://whois.icann.org (ou https://lookup.icann.org/lookup), foi possível constatar que a empresa que hospeda o *site* investigado [indicar URL] é a empresa X e a que oferece serviços de privacidade é a empresa Y.

De tal forma, a empresa X é a que hospeda o *site* malicioso e é quem possui os registros de criação do *site* e *logs* de acesso (IPs, data e hora). Por sua vez, a empresa Y é a que aparece como responsável pelo *site* malicioso no cadastro da empresa X de hospedagem e, portanto, deve ser interpelada para informar os dados do real responsável (dados cadastrais, inclusive financeiros) pelo site.

II) DO DIREITO

IIa) Da Ocorrência do Ilícito Eleitoral previsto no Art. X ....

Conforme visto no item I, o *site* [indicar URL] simula ser um *site* oficial do Governo Estadual, com o fim de angariar dados dos usuários e inocular códigos maliciosos, conforme se nota pelas imagens acima expostas.

[Descrição de detalhes do caso]

Assim evidencia-se que o responsável pelo mencionado *site* [detalhar a tipificação].

IIb) Da competência da Justiça Eleitoral

O artigo. , inciso da Constituição da República determina que a Justiça Eleitoral será competente para julgar ....

No caso concreto, a publicação menciona, expressamente, ...

IIc) Dos requisitos para a concessão da Medida Cautelar

Como é sabido, o direito à inviolabilidade da vida privada e da intimidade, previsto no art. 5º, incs. X e XII da Constituição Federal não se reveste de caráter absoluto, podendo e devendo ser relativizado quando indispensável para investigação criminal.

Nesse sentido, a Lei 12.965/14, conhecida como "Marco Civil da Internet", veio regulamentar especificamente o acesso aos registros de conexão ou de registros de acesso a aplicações de internet para viabilizar a investigação de fatos delitivos, reproduzido na Resolução 23.610/2019, art. 40, *in verbis*:

Art.40. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial, em caráter incidental ou autônomo, requerer ao juiz eleitoral que ordene ao responsável pela guarda o fornecimento dos dados constantes do art. 39 desta Resolução.
§ 1º. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade (Lei nº 12965/2014, art.22).
I - fundados indícios da ocorrência do ilícito de natureza eleitoral;
II - justificativa motivada da utilidade dos dados solicitados para fins de investigação ou instrução probatória; e
III - período ao qual se referem os registros.

Tomando-se por base os parâmetros estabelecidos na Lei n. 12.965/14, *in casu*, e na Resolução TSE 23.610/2019, consideram-se preenchidos os requisitos para o afastamento do sigilo telemático.

Como visto, há indícios razoáveis da prática da conduta ilícita tipificada no art. XX do . Necessário, neste ponto, identificar a autoria, partindo-se da individualização dos responsáveis pela publicação do conteúdo.

Ademais, a medida é necessária para a investigação dos fatos, já que possibilitará a colheita de elementos probatórios para a identificação da autoria do ilícito eleitoral.

Por fim, quanto à delimitação temporal exigida pelo legislador, tal requisito restou cumprido, já que se pretende a obtenção dos registros referentes ao período da criação do perfil investigado, bem como da publicação com conteúdo ilícito.

Assim sendo, estão presentes os requisitos necessários à quebra de sigilo telemático.

Como visto no item 1.2 desta peça, a empresa que hospeda o *site* investigado [indicar URL] é a empresa X e a que oferece serviços de privacidade é a empresa Y.

Outrossim, tendo em vista que a mensagem veicula conteúdo ilícito, é imprescindível seja determinada a sua remoção da plataforma virtual, até mesmo para cessar os efeitos nocivos no meio social.

III) DO PEDIDO

Ante o exposto, o MINISTÉRIO PÚBLICO ELEITORAL requer seja deferida a quebra de sigilo de dados telemáticos acima pleiteada, requerendo o que segue:

a) seja oficiada a empresa X, situada no endereço XXX, para que:

- forneça os dados de cadastros do responsável pelo *site* [indicar URL],
- forneça os *Logs* de criação do mencionado *site* (IP, data, hora e fuso horário);
- forneça os *Logs* de acesso ao site do período XX (Data em que se teve a notícia do funcionamento do *site*) até o recebimento do presente.
- remova o *site* [indicar URL] da Internet;
- não comunique ao responsável pelo site a presente medida, tendo em vista que o sigilo é necessário ao bom êxito das investigações; e que a resposta seja encaminhada com código *hash*.

b) seja oficiada a empresa Y, situada no endereço XXX, para que:

- forneça os dados cadastrais referente ao responsável pelo site [indicar URL];
-forneça os dados financeiros referente ao responsável pelo site (INDICAR URL), com a indicação da forma de pagamento, conta bancária, etc;
- não comunique ao ao responsável pelo *site* a presente medida, tendo em vista que o sigilo é necessário ao bom êxito das investigações e que a resposta seja encaminhada com código *hash*.

Com o objetivo de assegurar o prosseguimento das investigações, requer o Ministério Público Eleitoral a DECRETAÇÃO DO SIGILO ABSOLUTO DOS PRESENTES AUTOS.

Local e data.
XXXXXXXXXXXXXXX

Promotor (a) de Justiça Eleitoral

XIV) MODELO DE PEÇA DE MEDIDA CAUTELAR DE QUEBRA DE SIGILO TELEMÁTICO AO FACEBOOK

EXCELENTÍSSIMO SR. JUIZ ELEITORAL DA ___Nº ZONA ELEITORAL ...

SIGILOSO

Procedimento nº:

O MINISTÉRIO PÚBLICO ELEITORAL, pelo (a) Promotor (a) de Justiça Eleitoral, que ao fim assina, com fulcro em suas atribuições constitucionais e legais, vem à presença de Vossa Excelência requerer, com fulcro no artigo 5º, inciso XII, da Constituição Federal e no artigo 10, § 1º, da Lei 12.965/14 e artigo 39, da Resolução TSE nº 23610/2019, MEDIDA CAUTELAR DE QUEBRA DE DADOS TELEMÁTICOS, pelos motivos de fato e direito abaixo expostos:

I – DOS FATOS

O procedimento, em epígrafe, foi instaurado para apurar a possível prática do ilícito eleitoral tipificado no art. XXX do Código Eleitoral (ou da LC 64/1990) .

Conforme consta na notícia, o usuário do Facebook denominado XXX, com endereço eletrônico (URL - rodapé: URL (Uniform Resource Locator) é a forma padronizada de representação de diferentes documentos, mídias e serviços de rede na Internet, que identifica de forma completa cada documento com um endereço único. Ex. http://www.uol.com.br/serviços.php) no http://www.facebook.com/profile.php?id=1000000XXXXXXXX, publicou, em página do referido provedor de aplicação, no dia X, a seguinte mensagem, acessível na url www.facebook.com/xxxx):

[Reproduzir aqui a publicação ilícita]

Frente a tal informação, solicitou-se a preservação dos registros referentes à conta do perfil de XXX perante o Facebook (v. fl.), bem como solicito-se junto à Divisão Especial de Inteligência Cibernética do MP/RJ realizasse a colheita da prova, com extração do cálculo *hash*, o que foi cumprido, conforme fls. X.

A captura de tela da referida mensagem encontra-se em fl. X e, pela sua leitura, é possível notar que esta veicula conteúdo ilícito, subsumível à conduta típica prevista no art. XXX do .

Dessa forma, revela-se imperiosa, para a elucidação do delito penal sob investigação, a quebra de sigilo de dados telemáticos do usuário do perfil X, de modo a viabilizar sua identificação e reunir elementos probatórios acerca da prática criminosa investigada.

II) DO DIREITO

IIa) Da Ocorrência do Ilícito Eleitoral previsto no art. XXX do Código Eleitoral (ou LC

64/1990)

[Descrição dos fatos tais como apurados e tipificação]

IIb) Da competência da Justiça Eleitoral

O artigo , inciso , da

No caso concreto, a publicação menciona, expressamente, [identificar os pontos concretos que justificam a competência eleitoral, como a utilização de programas, mensagens e logos da Prefeitura Municipal/do candidato ....].

IIc) Dos requisitos para a quebra de sigilo telemático

Como é sabido, o direito à inviolabilidade da vida privada e da intimidade, previsto no art. 5º, incs. X e XII da Constituição Federal não se reveste de caráter absoluto, podendo e devendo ser relativizado quando indispensável para investigação eleitoral.

Nesse sentido, o artigo 22 da Lei 12.965/14, conhecida como "Marco Civil da Internet", veio regulamentar especificamente o acesso aos registros de conexão ou de registros de acesso a aplicações de internet para viabilizar a investigação do ilícito eleitoral, reproduzido na Resolução 23.610/2019, art.40, *in verbis*:

Art. 40. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de dados constantes do art. 39 desta Resolução.
§ 1º. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
I - fundados indícios da ocorrência do ilícito de natureza eleitoral;
II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
III - período ao qual se referem os registros.

Tomando-se por base os parâmetros estabelecidos na Lei n. 12.965/14, *in casu*, previstos na Res. TSE 23.610/2019, consideram-se preenchidos os requisitos para o afastamento do sigilo telemático.

Como visto, há indícios razoáveis da prática da conduta delituosa tipificada no art. XXX do Código Eleitoral (ou LC 64/90). Necessário, neste ponto, identificar a autoria, partindo-se da individualização dos responsáveis pela publicação do conteúdo.

Ademais, a medida é necessária para a investigação dos fatos, já que possibilitará a colheita de elementos probatórios para a identificação da autoria do ilícito eleitoral.

Por fim, quanto à delimitação temporal exigida pelo legislador, tal requisito restou cumprido, já que se pretende a obtenção dos registros referentes ao período da criação do perfil investigado, bem como da publicação com conteúdo ilícito.

Assim sendo, estão presentes os requisitos necessários à quebra de sigilo telemático.

Outrossim, tendo em vista que a mensagem veicula conteúdo ilícito, é imprescindível seja determinada a sua remoção da plataforma virtual, até mesmo para cessar os efeitos nocivos no meio social.

III) DO PEDIDO

Ante o exposto, o MINISTÉRIO PÚBLICO ELEITORAL requer seja deferida a quebra de sigilo de dados telemáticos acima pleiteada, com a expedição de ofício à empresa FACEBOOK INC, sediada em 1601 Willow Road, Menlo Park, CA 94025, United States, a/c FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA, CNPJ 13.347.016/0001-17, sediada na Rua Leopoldo Couto de Magalhães Júnior, 700, 5º Andar, Itaim Bibi, CEP 04542-000, São Paulo-SP[59] para que:

a) informe os dados cadastrais do usuário do perfil X [indicar URLs das contas com o número de identificação de usuário (ex: http://www.facebook.com/profile.php?id=1000000XXXXXXXX) e/ou com o nome de usuário (ex:http://www.facebook.com/nomedeusuario) do perfil do Facebook e/ou b) endereço de email e/ou c) o número de telefone (+55, DDD, número)]; inclusive nome visível, endereços eletrônicos e telefone vinculados à conta;
b) informe o e-mail ou número de terminal telefônico utilizado para a validação da criação da conta referente ao mencionado perfil;
c) informe os logs de acesso (contendo IP, data, hora e fuso horário) de criação do mencionado perfil;
d) informe os logs de acesso (contendo IP, data, hora e fuso horário) para a veiculação da mensagem referente à URL [indicar URL específica da publicação];
e) informe os logs de acesso (contendo IP, data, hora e fuso horário) do período de XX até a data da assinatura da ordem;
f) remova o conteúdo da publicação referente à URL [indicar URL específica da publicação], bem como os compartilhamentos desta mensagem;
g) não comunique ao usuário da conta investigada a presente medida, tendo em vista que o sigilo é necessário ao bom êxito das investigações.
h) que a resposta seja encaminhada com código *hash*.

Com o objetivo de assegurar o prosseguimento das investigações, requer o Ministério Público Federal a DECRETAÇÃO DO SIGILO ABSOLUTO DOS PRESENTES AUTOS.

Local e data.

XXXXXXXXXXXXXXXX
Promotor (a) de Justiça Eleitoral

59 Para encaminhamento do ofício por meio eletrônico, deve-se acessar o site https://www.facebook.com/records.

XV) MODELO DE OFÍCIO PARA PRESERVAÇÃO DE REGISTROS E REMOÇÃO DE SITE ILÍCITO PARA SERVIÇO DE HOSPEDAGEM

OFÍCIO n. Localidade, data de 2020.

URGENTE/SIGILOSO

Ao Diretor(a)
UOL - Universo On Line S/A
Rua Barão de Limeira, 458, Centro- São Paulo - CEP 01202 (ofício encaminhado pelo email intimauol@uolinc.com)

REF: REQUISIÇÃO DE PRESERVAÇÃO DE DADOS E PEDIDO DE REMOÇÃO DE SITE ILÍCITO
PROCEDIMENTO N.:

Senhor(a) Diretor (a),

O MINISTÉRIO PÚBLICO ELEITORAL, pelo(a) Promotor(a) de Justiça Eleitoral abaixo subscrito(a), comunico que foi instaurado o procedimento, em epígrafe, com o fim de investigar o *site* hospedado no endereço eletrônico:

[INDICAR A URL COMPLETA DO SITE].

O mencionado *site* simula ser um site oficial para (ex. angariar dados dos eleitores e inocular códigos maliciosos).

Assim, para instrução do procedimento supra identificado, com fundamento no art. 15, § 2º da Lei nº 12.965/2014 (Marco Civil da Internet) e art. 39 da Resolução TSE 23.610/2019, requisita-se a preservação dos seguintes dados referentes ao mencionado *site*:

- Dados de cadastros do responsável pelo site, inclusive informações financeiras;
- *logs* de criação do *site* (IP, data, hora e fuso horário);
- *logs* de acesso ao *site* do período XX (Data em que se teve a notícia do funcionamento do site) até o recebimento do presente.

Outrossim, tendo em vista que, através do mencionado *site*, é realizada atividade ilícita eleitoral, o que provavelmente contraria as normas de serviço desta empresa, solicita-se a remoção do *site* (indicar) da rede de Internet.

Outrossim, informo que, dentro do prazo legal, será realizado o ajuizamento de Medida Cautelar de Quebra de Sigilo Telemático para obtenção de ordem judicial para o envio dos registros e remoção do site, cuja preservação ora é solicitada.

Por fim, solicito que o presente pedido não seja informado ao usuário da conta, tendo em vista que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XXXXXXXXXXXXXXXXX
Promotor (a) de Justiça Eleitoral

MPF Ministério Público Federal | Procuradoria Regional Eleitoral no Rio de Janeiro

XVI) MODELO DE OFÍCIO PARA PRESERVAÇÃO DE REGISTROS E REMOÇÃO DE SITE ILÍCITO PARA SERVIÇO DE PRIVACIDADE

OFÍCIO n. Localidade, data de 2020.

URGENTE/SIGILOSO

Ao Diretor(a)

REF: PEDIDO DE PRESERVAÇÃO DE DADOS
PROCEDIMENTO N.:

Senhor(a) Diretor (a),

Para instrução do procedimento supra identificado, com fundamento no art. 13, § 2º e art. 15, § 2º da Lei nº 12.965/2014 (Marco Civil da Internet) e art. 39 da Resolução TSE 23.610/2019, venho por meio deste requisitar a preservação de dados cadastrais (inclusive dados financeiros) referentes ao *site* abaixo indicado, no período de XX (data da informação de funcionamento do *site*) até o momento do recebimento do presente ofício:

[URL DO SITE INVESTIGADO]

Outrossim, informo que, dentro do prazo legal, será realizado o ajuizamento de Medida Cautelar de Quebra de Sigilo Telemático para obtenção de ordem judicial para o envio dos registros (inclusive financeiro), cuja preservação ora é solicitada.

Por fim, solicito que o presente pedido não seja informado ao usuário da conta, tendo em vista que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XXXXXXXXXXXXXXXXX
Promotor(a) de Justiça Eleitoral

MPF Ministério Público Federal | Procuradoria Regional Eleitoral no Rio de Janeiro

XVII) MODELO DE OFÍCIO DE REQUISIÇÃO DE DADOS CADASTRAIS E DE PRESERVAÇÃO PARA PROVEDOR DE CONEXÃO (Claro S/A)

OFÍCIO n. Localidade, data de 2020.

URGENTE/SIGILOSO

Ao (À) Ilmo. (a) Senhor (a)
Diretor da
CLARO S/A, CNPJ n. 40.432.544/0001-47
Rua Verbo Divino, nº1.356, Chácara Santo Antônio, São Paulo/SP,
CEP 04.719-002 (*email* de encaminhamento: oficios.doc@claro.com.br)

REF: Requisição de dados cadastrais e preservação de conta
PROCEDIMENTO N.:

Senhor(a) Diretor (a),

Para instrução do procedimento, em epígrafe, instaurado para investigação de XX, venho, por meio deste, requisitar a Vossa Senhoria, com fundamento no art. 10, § 3º, da Lei nº 12.965/2014 (Marco Civil da Internet) e art. 39 da Resolução TSE 23.610/2019, o fornecimento, no prazo de [de 24 horas a 5 dias], dos dados cadastrais disponíveis do usuário vinculado à seguinte conexão:

- [indicação do IP, com DATA e HORÁRIO GMT].

Outrossim, solicito que sejam preservados os dados do mencionado usuário, referente ao período XX.

Solicito, ainda, que a resposta ao ofício: a) tenha caráter sigiloso, b) indique o número do procedimento em epígrafe e do presente ofício; c) seja encaminhada, em meio informatizado, com código *hash*, em arquivos que possibilitem a migração de informações para os autos do processo sem redigitação, nos termos do art. 7º, § 2º, da Resolução nº 181/2017-CNMP e d) seja enviada ao e-mail eletrônico XX.

Por fim, solicito que o presente pedido não seja informado ao usuário, tendo em vista que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XXXXXXXXXXXXXXXXX
Promotor (a) de Justiça Eleitoral

MPF Ministério Público Federal | Procuradoria Regional Eleitoral no Rio de Janeiro

XVIII) OFÍCIO DE SOLICITAÇÃO DE REMOÇÃO DE CONTEÚDO A PROVEDOR DE APLICAÇÃO (FACEBOOK)

OFÍCIO n. Localidade, data de 2020.

URGENTE/SIGILOSO

Ao
FACEBOOK INC
1601 Willow Road, Menlo Park, CA 94025, United States
A/C FACEBOOK/INSTAGRAM BRASIL
Rua Leopoldo Couto de Magalhães Júnior, 700, 5º Andar, Itaim Bibi,
São Paulo-SP - CEP 04542-000 (encaminhado pelo e-mail records@fb.com)

REF: PEDIDO DE REMOÇÃO DE CONTEÚDO
PROCEDIMENTO N.:

Senhor(a) Diretor (a),

Comunico a Vossa Senhoria que o MINISTÉRIO PÚBLICO ELEITORAL, por intermédio do(a) Promotor(a) de Justiça Eleitoral, que esta subscreve, recebeu a informação de que o usuário abaixo indicado, através de conteúdo publicado na rede social FACEBOOK e acessível na URL descrita a seguir, praticou conduta XX e, portanto, possivelmente violou normas contidas nos termos de uso desse provedor de aplicação.

Assim sendo, solicito a imediata adoção das providências necessárias à remoção do conteúdo indicado na URL abaixo, bem como da preservação dos dados referentes à página do perfil que segue:

- Identificação do conteúdo: www.facebook.xxx.
-Identificação da conta: http://www.facebook.com/profile.php?id=1000000XXXXXXXX OU http://www.facebook.com/username OU endereço de e-mail OU número de telefone no formato (+55, DDD, número).

Por fim, solicito que o presente pedido não seja informado ao usuário, tendo em vista que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XXXXXXXXXXXXXXXXXX
Promotor (a) de Justiça Eleitoral

MPF Ministério Público Federal | Procuradoria Regional Eleitoral no Rio de Janeiro

XIX) OFÍCIO DE SOLICITAÇÃO DE PRESERVAÇÃO DE DADOS A PROVEDOR DE APLICAÇÃO/CONEXÃO

OFÍCIO n. Localidade, data de 2020.

URGENTE/SIGILOSO

Ao Diretor(a)
Globo Comunicações e Participações SA
Rua Afrânio de Melo Franco, 135 - 5.o andar
Cep: 22430-060 - Leblon - RJ
Telefone: (21) 2540-4400

REF: PEDIDO DE PRESERVAÇÃO DE DADOS
PROCEDIMENTO N.:

Senhor(a) Diretor (a),

Para instrução do procedimento supra identificado, com fundamento no art. 13, § 2º e art. 15, § 2º da Lei nº 12.965/2014 (Marco Civil da Internet), venho por meio deste requisitar a preservação de dados referentes a conta abaixo indicada, no período de XX (data da publicação) até o momento do recebimento do presente ofício:

[Indicação dos dados de individualização da conta]

Outrossim, informo que, dentro do prazo legal, será realizado o ajuizamento de Medida Cautelar de Quebra de Sigilo Telemático para obtenção de ordem judicial para o envio dos registros, cuja preservação ora é solicitada.

Por fim, solicito que o presente pedido não seja informado ao usuário da conta, tendo em vista que o sigilo é necessário ao bom êxito das investigações.

Atenciosamente,

XXXXXXXXXXXXXXXXX
Promotor (a) de Justiça Eleitoral

XX) *Email* para a Polícia Federal como ponto de contato da rede 24X7

cybercrime_brazil_24x7@dpf.gov.br

De: Promotor de Justiça
Para: cybercrime_brazil_24x7@dpf.gov.br

Prezada Sra. Delegada de Polícia Federal,
Chefe do SRCC

Ref.: NF 1.34.001.00XXXX/2020-00

Solicito os bons préstimos dessa unidade para providenciar pedido de preservação de dados cadastrais, inclusive financeiros de pagamento do serviço (conta bancária, cartão de crédito ou relativos a carteira virtual, se o caso), dados de criação (IP, data e hora) e *logs* de acesso do site malicioso www.XXXJJJJ.com (INDICAR URL) que simula ser um *site* oficial do candidato/Partido/Prefeitura tal, com o fim de angariar dados dos usuários e inocular códigos maliciosos, conduta descrita no artigo XX, do Código Eleitoral (ou no art. 22 da LC 64/90)e que está hospedado pelo provedor (indicar nome da empresa provedora de hospedagem de sites) no país (indicar o país).

Ressalto a importância de que o usuário não seja notificado do pedido de preservação, até que seja obtida a devida ordem judicial de quebra de sigilo de dados telemáticos e enviado e cumprido o pedido de cooperação internacional para obtenção das informações cuja preservação ora se requer.

Aguardo a informação acerca dos dados que já puderem ser disponibilizados desde logo.

Atenciosamente,

XXXXXXXXXXXXXXXXX
Promotor (a) de Justiça Eleitoral

XXI) Fontes

Revista Exame: https://exame.abril.com.br/tecnologia/conteudo-digital-dobra-a-cada-dois-anos-no-mundo/.

http://pensando.mj.gov.br/marcocivil/pauta/neutralidade-de-rede-no-marco-civil-da-internet/); & MAGRANI, Eduardo. Democracia Conectada. Curitiba: Juruá, 2014.

Redes sociais influenciam voto de 45% da população, indica pesquisa do DataSenado (12 de dez. de 2019). Agência Senado.

Editorial do jornalista Tiago Sales, no artigo "O Combate às Fake News Em nome da verdade, edição da Revista Justiça e Cidadania, abril/2018.

Notícia TSE: http://www.tse.jus.br/imprensa/noticias-tse/2019/Maio/impacto-das-fake-news-em-eleicoes-mundiais-e-discutido-durante-seminario-no-tse.

Notícia STF: http://www.stf.jus.br/portal/cms/vernoticiadetalhe.asp?idconteudo=107402

Jornal Nexo: https://www.nexojornal.com.br/expresso/2020/03/16/O-que-as-redes-sociais-fazem-para-coibir-fake-news-em-meio-%C3%A0-pandemia

Notícia Senado: https://www12.senado.leg.br/noticias/materias/2020/02/17/uso-de-robos-para-influenciar-eleicoes-esta-na-pauta-da-ccj

Notícia TSE: http://www.tse.jus.br/imprensa/noticias-tse/2020/Maio/programa-de-enfrentamento-a-desinformacao-com-foco-nas-eleicoes-2020-mobiliza-instituicoes

Estadão: https://politica.estadao.com.br/noticias/geral,combate-as-fake-news-deve-incluir-sociedade,70003000272

Folha S. Paulo: https://www1.folha.uol.com.br/poder/2018/10/medir-impacto-de-fake-news-nas-eleicoes-e-dificil-diz-chefe-de-missao-da-oea.shtml

Uol: https://tab.uol.com.br/nova-bolha.

RUEDIGER, Marco Aurelio. Artigo: Os robôs nas redes sociais. FGV DAPP. http://dapp.fgv.br/artigo-os-robos-nas-redes-sociais/

CRUZ, Francisco Brito: Internet e Eleições no Brasil – Diagnóstico e Recomendações, 1a. ed., 2019/2020: https://www.internetlab.org.br/wp-content/uploads/2019/09/policy-infopol-26919_4.pdf

http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/25742/Desinforma%c3%a7%c3%a3o%20Policy-Paper-2%20Sala.pdf?sequence=1&isAllowed=y

BBC: https://www.bbc.com/portuguese/brasil-45666742

"Guia Prático sobre Combate à Desinformação e Investigação na Internet", do GACC da 2ª CCR do MPF

http://archive.icann.org/tr/portuguese.html.

Como funciona a internet ? Parte 1: O Protocolo IP: https://www.youtube.com/watch?v=HNQD0qJ0TC4

Como funciona a internet ? Parte 2: Sistemas Autônomos: https://www.youtube.com/watch?v=C5qNAT_j63M&t=41s

Como funciona a internet ? Parte 3: DNS: https://www.youtube.com/watch?v=ACGuo26MswI

Como funciona a internet ? Parte 4: Governança da Internet: https://www.youtube.com/watch?v=ZYsjMEISR6E

Notícia STF: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444265&ori=1

Estadão: https://link.estadao.com.br/noticias/empresas,alexandre-pede-vista-e-decisao-do-stf-sobre-bloqueio-ao-whatsapp-e-adiada,70003317970

https://internetsegura.br/coronavirus/

Jornal O GLOBO, "Em tempos de comoção, com fugir dos golpes na internet", edição de 30.03.2020.

BARRETO. Alessandro Gonçalves Barreto e Beatriz Silveira Brasil. Manual de Investigação Cibernética: À luz do Marco Civil da Internet. Brasport.

Aulas EAD da ESMPU sobre Investigação de Crimes Cibernéticos, de Fernanda Domingos.

https://portal.nucciber.mpba.mp.br/.

www.tre-rj.jus.br/site/eleicoes/2018/arquivos/cartilha_identificacao_usuarios.pdf.

www.trerj.jus.br/site/eleicoes/2018/arquivos/cartilha_localizacao_especificacao_conteudo.pdf

https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf.

https://cartilha.cert.br/fasciculos/verificacao-duas-etapas/fasciculo-verificacao-duas-etapas.pdf .

Agradecemos a Rodrigo Tamussino Roll e Yago Vasconcelos Falcão, alunos da graduação da FGV Direito Rio, pelo auxílio na pesquisa e texto dos capítulos I a IV deste guia.