MINISTÉRIO PÚBLICO FEDERAL
CÂMARA CRIMINAL
GRUPO DE APOIO SOBRE CRIMINALIDADE CIBERNÉTICA

FAKE NEWS e COMO INVESTIGAR

Neide M. C. Cardoso de Oliveira[1]
Silvana Batini Goés

Uma das grandes preocupações da sociedade digital hodiernamente é a propagação de notícias falsas. *Uma pesquisa do Instituto Tecnológico de Massachusets (MIT)*[2]*, 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.*

Assim como a Justiça Eleitoral está se preparando para combater este tema, que será um dos mais importantes desafios das eleições gerais de 2018, os procuradores eleitorais também devem ter noção de como agir no caso de eventuais denúncias, por exemplo, como a criação de dezenas ou centenas de perfis falsos em favor de um determinado candidatado às eleições gerais ou à ideologia de um determinado partido político. Normalmente, as notícias falsas são criadas intencionalmente por algum motivo seja ele político, econômico ou ideológico.

---

1 Neide M. C. Cardoso de Oliveira – procuradora Regional da República na PRR da 2ª Região, membro do Núcleo de Criminal de Combate à Corrupção – Força Tarefa Lava Jato da PRR2 e coordenadora do Grupo de Apoio sobre Criminalidade Cibernética da 2ª CCR Silvana Batini Góes - procuradora Regional da República na PRR da 2ª Região, membro do Núcleo de Criminal de Combate à Corrupção – Força Tarefa Lava Jato da PRR2, procuradora regional Eleitoral, no período de

2 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.

Em geral, divulgar boatos não é um ato criminoso, desde que o boato não caracterize os delitos de calúnia, difamação e injúria, previstos no Código Penal. Há também a possibilidade de a notícia caracterizar crime de racismo, previsto no art. 20, § 2º, da Lei 7718/89.

O Código Eleitoral prevê como crime a conduta de divulgar fatos inverídicos que possam influenciar no eleitorado, tipificando, também, de forma especial, os crimes de calúnia, difamação e injúria. Mas estes tipos estão atrelados ao ambiente da propaganda oficial dos candidatos.

E a experiência mostra que a ameaça mais séria das *fake news* não deve vir da propaganda oficial dos candidatos na internet. Mas da multiplicação de postagens e perfis clandestinos e falsos. Neste caso, desvinculados do contexto da propaganda, o enquadramento típico será o de crime comum e a competência, da justiça federal comum, e não eleitoral.

Já no âmbito estrito do Direito Eleitoral, a conduta de divulgar boatos pode caracterizar ilícitos eleitorais graves, aptos a comprometer o equilíbrio e a lisura do pleito. No ambiente aberto das redes sociais, não será surpresa se o período eleitoral incentivar o discurso de ódio e a mentira como ferramentas ilícitas da polarização que se apresenta, incidindo em diversas infrações eleitorais.

Neste contexto, a caracterização do ilícito do uso indevido dos meios de comunicação social, tradicionalmente atrelado às mídias convencionais, 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 constatação de que houve pagamento para impulsionamento de postagens contendo *fake news* deve caracterizar, de plano, o ilícito de abuso de poder econômico.

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.

O primeiro passo para se investigar uma notícia falsa divulgada na Internet é a **identificação do provedor de aplicações de internet**[3] (*Facebook, Twitter, Youtube/Google, WhatsApp*, *site* na *web*, etc), que publicou aquela notícia falsa/criminosa, e essa identificação é feita nos *sites* do www.registro.br ou *whois* (informa se provedor está no exterior), se não for de fácil percepção.

Em seguida, deve ser solicitado junto ao provedor de aplicativo identificado, a **preservação de todos os elementos referentes àquela publicação falsa/criminosa** (com identificação do **nome da URL**[4] **ou ID**[5] correta do perfil, de um grupo; de um vídeo etc)[6]. Essa identificação exata é essencial para que a empresa de internet identifique corretamente nos seus serviços a publicação, que está sendo pedida preservação, e o correspondente usuário, que a publicou. Não é suficiente o nome do Perfil, por exemplo, no caso do *Facebook* ou envio de uma imagem, obtida com um *snapshot* da tela. A correta identificação da publicação é o maior entrave para o início de qualquer investigação na Internet, pois sem a URL ou ID, a empresa não tem como localizar o perfil, site ou grupo. O pedido de preservação da notícia pode ser feito diretamente pelo Ministério Público ao

3 Alterada nomenclatura, em 26.06.2018.

4 URL (Uniform Resource Locator) que é a forma padronizada de representação de diferentes documentos, mídias e serviços de rede na Internet, que identifica cada documento com um endereço único.

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

6 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

A URL de um vídeo específico: https://www.youtube.com/whatch/v=2y-5hfZWADI

provedor de aplicações de Internet porque não se está pedindo qualquer dado, apenas solicitando que a empresa preserve aquela publicação e seus dados respectivos para posterior envio de uma ordem judicial. Esse pedido deve ser feito o mais breve possível, porque muitas vezes, o usuário a retira logo da Internet e sem a publicação e sua identificação não é possível iniciar uma investigação.

Após, 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, do Marco Civil da Internet, para que o Juízo respectivo requisite do provedor de aplicação à Internet as informações de IP (*Internet Protocol Address*)[7] de criação, data e hora do (s) texto (s) ou imagem (ns) postada (s), identificado pela URL ou ID, bem como demais *logs* (que são registros) de acesso; outras informações relacionadas, como e-mail e eventual (is) vídeo (s) ou imagem (ns) publicadas naquele provedor, para configurar a materialidade.

Com o envio dessas informações, pelo número do IP indicado pelo provedor de aplicações, é possível **identificar o provedor de conexão (as operadoras de telefonia ou telecomunicações, que ofereçam banda larga**), a partir de um consulta no site http://registro.br[8] ou whois (informa os endereços de IPs no exterior). É possível requisitar diretamente ao provedor de conexão os dados cadastrais do usuário investigado, de acordo com o artigo 10, § 3º, do Marco Civil da Internet, no entanto, algumas operadoras ainda só fornecem esses dados cadastrais mediante ordem judicial e, nos casos criminais, pode ser mais prudente (novo requerimento de afastamento de sigilo telemático dirigido à empresa de telefonia, detentora daquele IP). A operadora indicará o endereço do titular da conta, onde estará o dispositivo, seja ele um terminal de computador, celular etc, que divulgou aquela notícia.

---

7 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.

8 No Brasil, o NIC.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.

A providência seguinte, **no caso de investigação criminal**, é a **medida cautelar de busca e apreensão** (art. 240, § 1º, alínea "e" e "h", do CPP) do material divulgado, apreendendo-se o dispositivo para posterior perícia. Não há legislação específica para quando essa medida se destinar à apuração de um crime praticado pela Internet, por isso são utilizadas as normas referentes à busca e apreensão previstas no Código de Processo Penal.

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

A dúvida surge quanto à arquivo armazenado "nas nuvens", isto é, servidores remotos, instalados em local diverso de onde o equipamento deve ser apreendido. 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, os agentes, cumpridores da diligência de busca e apreensão, podem acessar e coletar esses arquivos e toda evidência digital relacionada a eles.

Após a busca e apreensão, será necessária uma investigação simples, feita pela autoridade policial ou ministerial, visando identificar a autoria, caso residam mais de uma pessoa no local onde foi apreendido o dispositivo, entre moradores, por exemplo, sobre quem utilizava o computador ou se um terceiro estranho à residência o utilizava, salvo nos casos de apreensão de celular, apreendido com o próprio investigado.

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, **não há necessidade de busca e apreensão da notícia que já é pública**. Basta a identificação do usuário do IP, que se conectou à Internet, por determinado dispositivo e fez a referida publicação.

Os grandes provedores de aplicativos à Internet, que prestam serviços no País, como

Facebook[9] e *Twitter*[10], comunicaram que estão se preparando para as eleições gerais no Brasil, dizem que deletam perfis falsos, fazem campanhas sobre *fake news* e colaboram com as autoridades. È necessário também o aperfeiçoamento de ferramentas no próprio aplicativo, que identifiquem os robôs, utilizados para propagar *fake news* em seus serviços. Nos EUA, o *Facebook* criou o programa denominado "*Trust*", durante as eleições presidenciais americanas, com o objetivo de identificar tais *fake news*, no entanto, segundo as notícias sobre ele[11], o mesmo não funcionou.

9 http://agenciabrasil.ebc.com.br/geral/noticias/2017-12/0-que-diz-o-facebook-em-relacao-fake-news
10 Reunião realizada na sede da PR/SP, em 25.04.2018, com representantes do Twitter, Vice-PGE e membros do GACC.
11 http://www.folha.oul.com.br/mercado/2017/12/1944695-test-do-facebook-afeta-mais-a-midia-profissional-que-fake-news.shtml