

FAKE NEWS E UTILIZAÇÃO DE FONTES ABERTAS

Alesandro Gonçalves Barreto¹

RESUMO

A disseminação de notícias falsas, de maneira instantânea e em velocidades inimagináveis, através de sites, redes sociais e aplicativos de mensageria, e em velocidades inimagináveis, têm gerado várias preocupações para os operadores do direito, dentre as quais, a confirmação de integridade do conteúdo. Algumas agências têm se destacado nessa identificação, especialmente as de “fact checking”. Procuraremos, para tanto, assinalar ferramentas livremente disponíveis na Internet de verificação de integridade, não esgotando, contudo, outros recursos ora acessíveis.

Palavras-chave: Fake News; Fontes; Internet.

INTRODUÇÃO

A potencialização da *Internet* e suas funcionalidades têm trazido inúmeras possibilidades, seja para usuários ou para empresas. A cada instante somos apresentados a novas possibilidades, sendo inundados por novas informações que, por vezes, tornam difícil distinguir fato de ficção.

Esse cenário tem facilitado a divulgação de notícias falsas por sites, blogs, redes sociais e aplicativos de mensageria, possibilitando a propagação de *fake news* de maneira instantânea e em velocidades até então inimagináveis.

Ademais, o uso de robôs potencializa esse compartilhamento através de contas automatizadas. Segundo estudo realizado pela Diretoria de Análise de Políticas Públicas da Fundação Getúlio Vargas – FGV-DAPP, essas contas automáticas possibilitam a ampla divulgação de postagens e são uma ferramenta em potencial para a manipulação dos debates nas redes sociais. Ainda de acordo com o trabalho empreendido pela FGV, “na greve geral de 2017, mais de 20% das interações ocorridas no Twitter entre usuários a favor da greve foram provocados por esse tipo de conta”¹.

Assistimos, nos últimos anos, ao crescimento desse comportamento, especialmente na questão eleitoral. Nas eleições presidenciais estadunidenses de 2016, tivemos várias notícias

¹ Delegado de Polícia Civil do Estado do Piauí e co-autor dos livros *Inteligência Digital*, *Manual de Investigação Cibernética* e *Investigação Digital em Fontes Abertas*, da Editora Brasport, Vingança Digital, Mallet Editora. delbarreto@gmail.com.



falsas veiculadas sobre as candidaturas. O mesmo fenômeno ocorreu na França, onde circularam *fake news* sobre os candidatos, culminando posteriormente com um projeto de lei para criminalizar os responsáveis por esse tipo de condutaⁱⁱ.

A confiança na tela do dispositivo informático é combustível para esse cenário. GOODMAN (2015) pontua sobre a confiança irrestrita que temos no conteúdo que nos é oferecido na *Internet*, ressaltando queⁱⁱⁱ:

O entra lixo, sai lixo, foi suplantado pelo entra lixo, sai evangelho: se o computador está dizendo isso, então deve ser verdade. O problema com esse raciocínio é que nós, como sociedade, estamos confiando em dados incorretos o tempo todo, um problema desagradável que se voltará contra nós. Bolhas de filtro, censura invisível em ferramentas de busca, firewalls nacionais e dados incorretos significam que temos um problema de integridade fundamental com nossa maneira de ver o mundo o, mais precisamente, com a maneira como o mundo nos é apresentado e mediado por nossas telas.

Em 2018, quando serão eleitos os representantes brasileiros no executivo e legislativo nos níveis federal e estadual, sem sombras de dúvidas os cidadãos conectados em redes sociais serão inundados por notícias com o intuito de desvirtuar o processo eleitoral em comentário. Todavia, não poderemos ficar adstritos apenas ao aspecto eleitoral, eis que a propagação de notícias falsas pode ensejar a prática de crimes tipificados no Código Penal Brasileiro ou na legislação extravagante.

Segundo BUTRY (2014), é preciso ao relatar a necessidade de verificação da autenticidade dos fatos que são difundidos. Estabelece também a mistura de três fatores para essa checagem: 1) habilidade, persistência e ceticismo profissional; 2) conhecimento, honestidade e confiabilidade e variedade da fonte, e; 3) documentação; asseverando que^{iv}:

A tecnologia mudou a forma de como aplicamos esses três fatores: o ciclo de notícias de 24h e a ascensão das mídias sociais e dos conteúdos gerados por usuários exigem que façamos a apuração e divulgação das notícias ao mesmo tempo em que os eventos acontecem, decidindo rapidamente se uma informação foi suficientemente verificada; ferramentas digitais nos oferecem novas formas de encontrar e contatar fontes; bancos de dados e os onipresentes celulares com câmeras nos fornecem quantidades altíssimas de documentação. Uma verificação bem-sucedida resulta do uso eficaz da tecnologia, assim como do comprometimento com padrões imutáveis de precisão.



O volume de dados trafegados na *Internet* por minuto torna incapaz seu processamento apenas pelo homem, necessitando a aplicação de inteligência artificial, agregada ao aprendizado de máquina para verificação da autenticidade de uma notícia. Não obstante, a coleta de dados disponíveis na rede mundial de computadores, através da inteligência de fontes abertas, garantirá ao utilizador, nas mais diversas situações, mecanismos para responder sobre um fato, tais como: autenticidade, data e local de criação, perfis em redes sociais, provedor de hospedagem (nome e dados para contato), responsável pelo *upload* e uma linha do tempo de sua divulgação, dentre outras.

1. UTILIZAÇÃO DE FONTES ABERTAS

O incremento dos avanços tecnológicos produz uma quantidade de dados de livre acesso que, em razão dessa disponibilidade, podem ser úteis na verificação da autenticidade de uma notícia que viralizou em redes sociais. Poderíamos citar, como exemplo, uma situação de greve dos órgãos de segurança pública, sobre a qual circulam imagens e textos atribuindo aqueles acontecimentos à paralisação. Em alguns casos, uma rápida procura em ferramentas de pesquisa por textos e imagens reversas demonstrará, de pronto, que aquele conteúdo já havia sido publicado em local e circunstância distinta.

BARRETO, CASELLI e WENDT (2017) definem fontes abertas como^v:

Qualquer dado ou conhecimento que interesse ao profissional de inteligência ou de investigação para a produção de conhecimentos e ou provas admitidas em direito, tanto em processos cíveis quanto em processos penais e, ainda, em processos trabalhistas e administrativos (relativos a servidores públicos federais, estaduais e municipais).

CEPIK (2003) enfatiza o livre acesso da informação na inteligência de fontes abertas, explanando-a como:

A obtenção legal de documentos oficiais sem restrição de segurança, da observação direta e não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia, da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, de um leque mais ou menos amplo de fontes disponíveis cujo acesso é permitido sem restrições especiais de segurança.



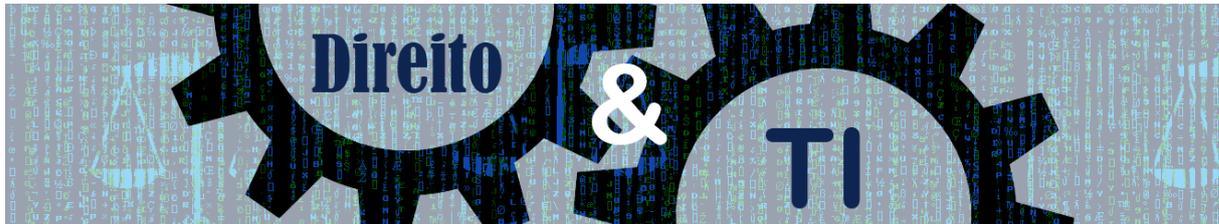
À vista disso, procuraremos demonstrar algumas técnicas a serem utilizadas nessa verificação. Recomendamos, por oportuno, a utilização das ferramentas de fontes abertas em duplicidade. Outrossim, ressaltamos que não se tratam de procedimentos exaustivos, apenas servem como caminho para averiguação de um fato, devendo ser confrontados com outras fontes de dados disponíveis.

1.1 Das Ferramentas de Busca

As ferramentas de busca devem ser utilizadas como mecanismo de verificação de um fato. Podemos utilizá-las para encontrar notícias relacionadas, imagens semelhantes, tópicos relacionados, dentre outros. Muito embora alguns dados possam não ser confirmados com esse procedimento, noutras situações podemos, de imediato, detectar que se trata de *fake news*.

O Google pode ser utilizado na checagem de informações que circulam em redes sociais e/ou serviços de mensageria. A ferramenta de busca possui uma diversidade de funcionalidades que podem, de início, auxiliar na detecção de *fake news*:

- a) Google Pesquisa^{vi} – Possibilita a busca de palavras-chave daquele fato veiculado. Para tanto, podemos utilizar várias técnicas de busca avançada: uso de aspas para localizar termos e frases específicas; em ferramentas e/ou configurações, poderemos filtrar os resultados para alcançar melhores resultados (país, idioma, data, todos os resultados); uso de hifens para excluir palavras; aplicação do caractere coringa “*” para fazer a substituição por outras palavras, dentre outras^{vii}.
- b) Google Imagens^{viii} – Proporciona a localização de imagens semelhantes na *Internet*, além de apontar os sites nos quais ela se encontra hospedada e outros tamanhos disponíveis da ilustração em apreço. A pesquisa pode ser feita utilizando a *url* da imagem, bem como fazendo seu download, arrastando a imagem e solta no campo de pesquisa do Google Imagem. TinyEye é uma ferramenta disponível que também pode ser utilizada para fazer essa constatação^{ix}. Outro caminho a ser seguido é checar o metadado da fotografia através de sites de livre acesso^x ou verificar se houve alguma alteração na imagem^{xi}.
- c) Google Alerts^{xii}- possibilita a criação de alertas e recebimento de notícias por *email*. No caso de uma notícia que está circulando, o usuário poderá acompanhar, através de



palavras-chave, assunto que eventualmente estejam sendo indexados pela ferramenta de busca. Como alternativa, podemos utilizar o TalkWalker Alerts^{xiii}.

- d) Google Trends- a sua utilização propicia encontrar os resultados sobre a busca de um termo num determinado período e região. Ao pesquisar sobre o tema *fake news*, por exemplo, percebemos que seu interesse se encontra em todos continentes^{xiv}.



Figura 1- Consulta ao Tema Fake News na ferramenta Google Trends em 31 de jan. 2018.

1.2 Repositórios e Verificadores de Boatos

A verificação de notícias falsas pode ser realizada por alguns sites disponíveis na Internet. Com a finalidade de identificar e contrapor os conteúdos acessíveis, esses repositórios funcionam como excelentes fontes de consulta, especialmente para o jornalismo nos assuntos da política nacional e internacional.

O site Hoaxy^{xv} examina o compartilhamento de *fake news* em mídias sociais, oportunizando fazer comparações em sites de verificação de notícias falsas do mesmo modo que identifica o compartilhamento de forma gráfica no Twitter. Apesar de estarem livremente



disponíveis, os resultados são mais precisos quando as palavras chaves são pesquisadas na língua inglesa.

O Projeto Snopes, disponível em <https://www.snopes.com>, foi fundado há mais de vinte anos tendo, com o propósito inicial a verificação de lendas urbanas, especializando-se na verificação de boatos online.

No Brasil, alguns sites dispõem dados sobre boatos que circulam na Internet. Essas aplicações podem ser utilizadas como ferramentas acessórias para identificação de *fake news*. Podemos elencar:

- <http://www.boatos.org/>
- <http://www.e-farsas.com/>
- <http://www.boatos.info/>

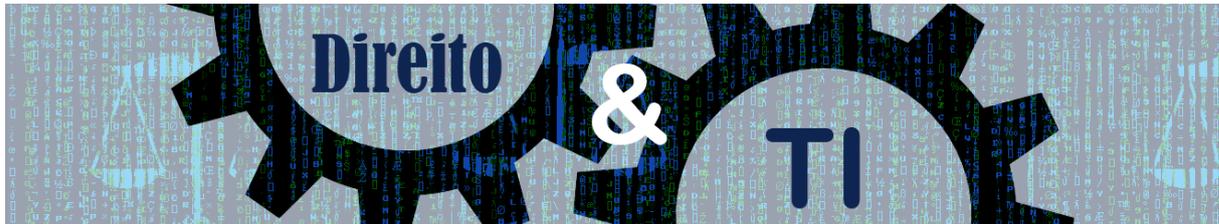
No exame de noticiais de mensagens em *smartphone* sobre atualização de dados bancários, recebimento de FGTS, promoções ou qualquer outro evento que tente induzir o internauta a clicar em links desconhecidos ou suspeitos, é possível fazer a verificação daquele conteúdo. O Catálogo de Fraudes da Rede Nacional de Ensino e Pesquisa, disponível em <https://www.rnp.br/servicos/seguranca/catalogo-fraudes>, viabiliza a consulta de informações sobre as fraudes que estão sendo cometidas diariamente.

1.3 Redes Sociais

As redes sociais, muito embora tenham sido criadas para realização de atividades lícitas e, em razão do seu alcance, têm seu propósito desvirtuado, sendo utilizadas para a divulgação de notícias falsas. Procuraremos fazer uma análise das principais redes sociais utilizadas.

1.3.1 Facebook

Algumas delas tem procurado implementar soluções para evitar essa propagação em suas plataformas. O Facebook, por exemplo, tem realizado mudanças nesse sentido. Para tanto, é possível fazer denúncias de um conteúdo nos casos de postagens que contenham links externos, não exequíveis nos casos de *upload* de fotos e vídeos realizados diretamente no perfil do usuário.



Ademais, o usuário que não seja classificado como veículo de mídia não será capaz de modificar dados de conteúdo ou características de uma imagem quando tentar compartilhar uma notícia. Essa mudança evitará a modificação de conteúdo de sites de notícias em buscas de cliques com o intuito de monetizar páginas.

O fluxograma abaixo demonstra o procedimento para realizar essa denúncia:

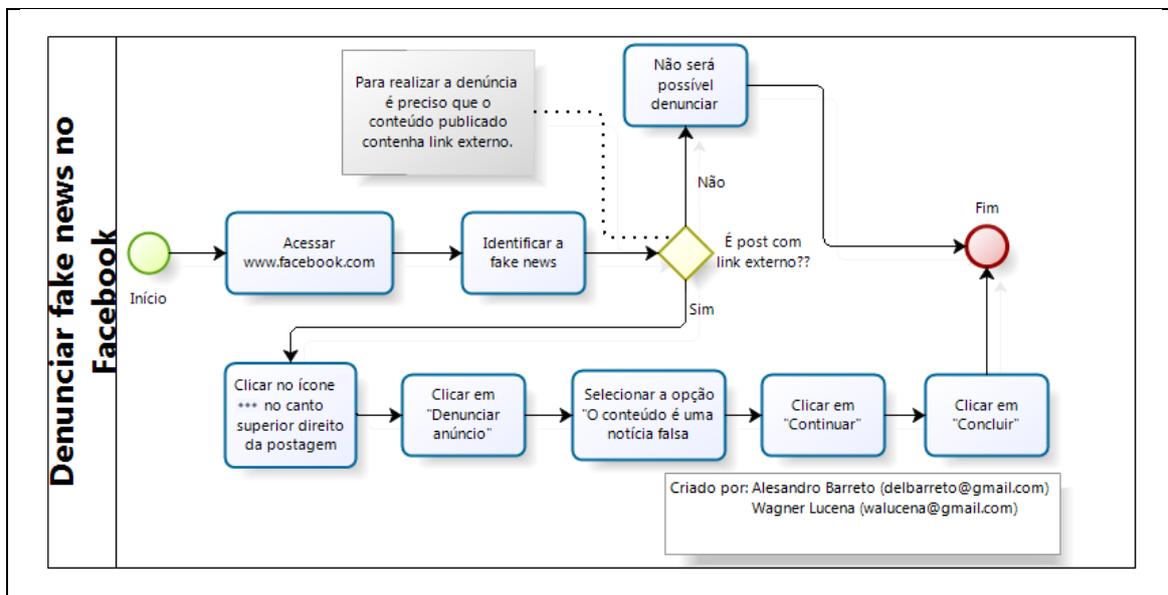
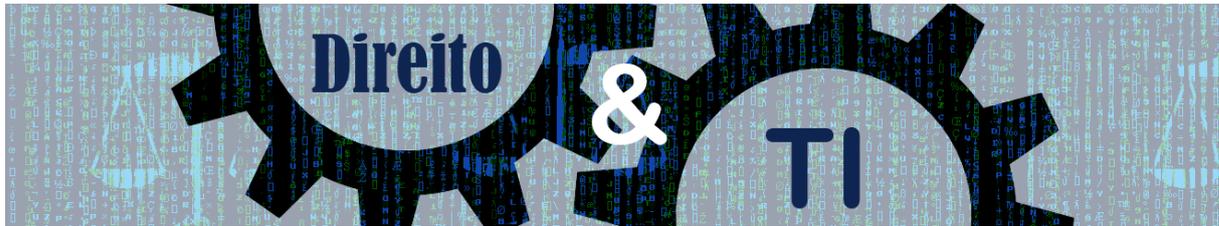


Imagem 02: Processo descritivo da realização de denúncia de notícia falsa junto ao Facebook

1.3.2 Twitter

Existem várias ferramentas disponíveis para checagem de notícias dentro da plataforma. O site Intel Techniques, exequível no link <https://inteltechniques.com/osint/twitter.html> oportuniza a consulta personalizada.

A busca por *hashtag* pode ser realizada diretamente na página do Twitter. Há, todavia, ferramentas para obter dados sobre popularidade, tendências e suas correlações. Ressalte-se, por oportuno, que a versão paga pode trazer mais funcionalidades e resposta sobre uma consulta. Podemos fazer essa consulta em: Hashtagify^{xvi} e Hashtag.org^{xvii}. No site <http://ctrlq.org/first/> através de palavras chaves ou de *links*, poderá encontrar o primeiro *tweet* que contém o termo procurado, ajudando a montar a linha do tempo do boato.



A ferramenta TweetDeck possibilita o acompanhamento de notícias em tempo real sobre o determinado assunto através de um *dashboard* interativo, indicando quais usuários estão postando naquele instante^{xviii}. O acompanhamento por assunto e por geolocalização^{xix} pode ser realizado pelo Twitterfall^{xx}.

Por vezes, esses compartilhamentos são realizados por contas robôs que, simulando o comportamento humano, interagem com usuários reais criando conteúdo ou interagindo em discussões em andamento. O site Botomoter permite verificar a atividade de uma conta no Twitter e apontar as probabilidades de ser um robô^{xxi}.

1.3.3 Youtube

No Youtube, por exemplo, a ferramenta Youtube Data Viewer, acessível em <https://citizenevidence.amnestyusa.org/>, faculta a busca de dados ocultos de vídeos que estejam hospedados na aplicação. Quando várias cópias de um mesmo vídeo estejam sendo divulgadas, é possível contrastá-las e precisar o tempo real em que cada uma foi carregada, sendo possível, em tese, determinar o primeiro usuário a carregar o conteúdo. Além de tudo, podemos encontrar vídeos mais antigos pesquisando com base na imagem reversa.

As denúncias por conteúdo enganoso podem ser realizadas diretamente na plataforma. Na parte inferior do vídeo basta clicar no ícone “...” – Denunciar - spam ou enganoso- texto enganoso ou golpe e fraude.

1.4 Sites

De quando em vez, a verificação de autenticidade de uma notícia pode ser checada com a obtenção de informações sobre o site, autoria da publicação e responsável pela hospedagem do conteúdo, devendo, todavia, esses dados serem confrontados com outros elementos de informação a fim de saber quais os propósitos de quem está por trás daquela publicação.

Em determinadas ocasiões, um fato foi divulgado, em primeira mão, por um site que foi registrado e hospedado apenas três dias atrás. Conseguiremos, utilizando ferramentas livremente disponíveis, informação sobre responsável pelo site, CPF ou CNPJ, data de criação e de expiração, *email* para contato, além do servidor de hospedagem. No cumprimento de decisão



judicial para suspensão da disponibilidade do serviço de determinado site, deve-se fazer o encaminhamento diretamente para este último.

Há várias ferramentas disponíveis para obtenção desses dados. Ao utilizar a ferramenta de busca do Google, basta utilizar a palavra-chave “whois”, que as opções estarão acessíveis. Citamos, como exemplo, Whois Registro BR, Geek Tools, Arin, DNSStuff, WhoisLookup e Who.is^{xxii}.

Caso tenha encontrado a data e o site da publicação, poder-se-á usar a plataforma “Wayback Machine”, disponível em <http://archive.org/web/>, para tentar obter a imagem das páginas armazenadas do sítio eletrônico.

CONCLUSÃO

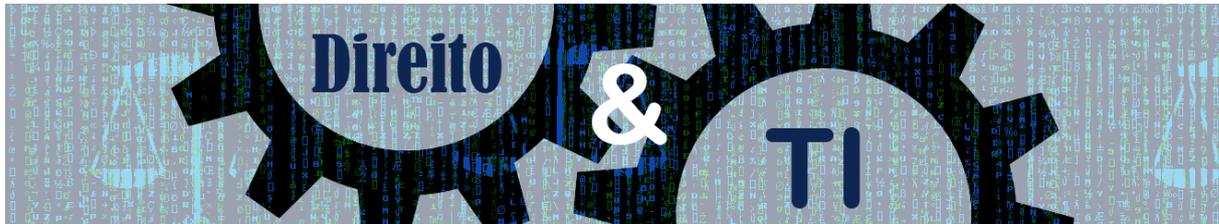
A utilização de fontes abertas é apenas um meio para verificação da integridade de uma informação que está circulando nas redes sociais, não sendo, todavia, o único procedimento a ser realizado. O volume de dados produzidos é imenso, não impossível de ser processado pelo ser humano.

Nesse contexto, a utilização de inteligência artificial e aprendizado de máquina (*machine learning*) permitirão realizar de tarefas visando detectar a circulação de notícias falsas na rede mundial de computadores.

Por outro lado, as aplicações de Internet, especialmente as redes sociais e os aplicativos de mensageria, têm papel relevante, devendo aperfeiçoar seus algoritmos para um enfrentamento eficaz do *fake news*.

Ademais, a agilidade na retirada das notícias falsas de suas plataformas, seja por ordem judicial, seja por violação às suas políticas de privacidade, impossibilita a disseminação numa maior escala, minimizando seus assoladores efeitos.

Sob outro ponto de vista, a educação digital poderá trazer cenários positivos para evitar a propagação de notícias não confirmadas. As devidas cautelas devem ser levadas em conta no momento de retransmitir fatos carregados de exageros ou sensacionalismos, tais como: “ninguém divulgou isso”; “urgente”; “não deixe de ler”; “atenção”; “não deixem de divulgar”; “bomba”, dentre outros termos que procuram transformar leitores desatentos em peças impulsionadoras de virais.



Em síntese, as ferramentas disponíveis em fontes abertas ora explanadas não são exaustivas na identificação dos virais, necessitando, pois, de adoção de um conjunto de medidas para restringir os efeitos danosos dessa prática.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. Manual de Investigação Cibernética à Luz do Marco Civil da Internet. Rio de Janeiro: Ed. Brasport, 2016.

_____. WENDT, Emerson. CASELLI, Guilherme. Investigação Digital em Fontes Abertas. BRASPORT Editora. Rio de Janeiro. 2017.

_____. Projetos de Lei criminalizando o jogo baleia azul: utilidade para a investigação policial? Disponível em: <<http://direitoeti.com.br/artigos/projetos-de-lei-criminalizando-o-jogo-baleia-azul-utilidade-para-a-investigacao-policial/>>. Acesso em: 10 fev. 2017.

_____. Emergency request disclosure: a polícia judiciária e as solicitações de emergência às aplicações de internet. Disponível em: <<http://direitoeti.com.br/artigos/emergency-request-disclosure-a-policia-judiciaria-e-as-solicitacoes-de-emergencia-as-aplicacoes-de-internet/>>. Acesso em: 10 fev. 2018.

_____. Fake News e criminalização da divulgação: seria esse o caminho?. Disponível em: <<http://direitoeti.com.br/artigos/fake-news-e-criminalizacao-da-divulgacao-seria-esse-o-caminho/>>. Acesso em: 10 fev. 2018.

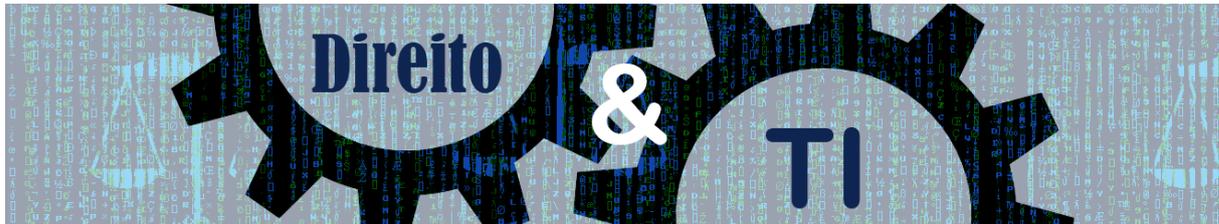
BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 fev. 2018.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 10 fev. 2018.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 10 fev. 2018.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp105.htm>. Acesso em: 10 fev. 2018.

Fundação Getúlio Vargas. ROBÔS, REDES SOCIAIS E POLÍTICA: ESTUDO DA FGV/DAPP APONTA INTERFERÊNCIAS ILEGÍTIMAS NO DEBATE PÚBLICO NA WEB. LEVANTAMENTO MOSTRA QUE CONTAS AUTOMATIZADAS MOTIVAM ATÉ 20% DE DEBATES EM APOIO A POLÍTICOS NO TWITTER, IMPONDO RISCOS À



DEMOCRACIA E AO PROCESSO ELEITORAL DE 2018. Disponível em <<http://dapp.fgv.br/robos-redes-sociais-e-politica-estudo-da-fgvdapp-aponta-interferencias-ilegitimas-no-debate-publico-na-web/>>. Acesso em: 09 fev. 2018.

GOODMAN, Marc. Future Crimes: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. HSM Editora, São Paulo, 2015.

ISTOÉ. Macron anuncia projeto de lei contra ‘fakenews’ em eleições. Disponível em <https://istoe.com.br/macron-anuncia-projeto-de-lei-contra-fake-news-em-eleicoes/>. Acesso em: 09 fev. 2018.

WENDT, Emerson. Internet & Direito Penal. Risco e Cultura do Medo. Porto Alegre: Ed. Livraria do Advogado, 2016.

ⁱ ROBÔS, REDES SOCIAIS E POLÍTICA: ESTUDO DA FGV/DAPP APONTA INTERFERÊNCIAS ILEGÍTIMAS NO DEBATE PÚBLICO NA WEB. LEVANTAMENTO MOSTRA QUE CONTAS AUTOMATIZADAS MOTIVAM ATÉ 20% DE DEBATES EM APOIO A POLÍTICOS NO TWITTER, IMPONDO RISCOS À DEMOCRACIA E AO PROCESSO ELEITORAL DE 2018.

ⁱⁱ ISTOÉ. Macron anuncia projeto de lei contra ‘fakenews’ em eleições.

ⁱⁱⁱ GOODMAN, Marc. Future Crimes: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. P. 143

^{iv} Steve Buttry. O básico da verificação: regras para seguir. P. 17. In: Manual de Verificação. Um Guia Definitivo para a Verificação de Conteúdo Digital na Cobertura de Emergências. Editado por Craig Silvermann. Traduzido pela Agência Paradox Center. European Journalism Center.

^v BARRETO, Alessandro Gonçalves; CASELLI, Guilherme; WENDT, Emerson. Investigação Digital em Fontes Abertas. Rio de Janeiro: Brasport, 2017.

^{vi} Disponível em <https://www.google.com.br/>.

^{vii} Como pesquisar no Google. Disponível em: <https://support.google.com/websearch/answer/134479?hl=pt-BR>.

^{viii} Google Images. Disponível em <https://www.google.com.br/imghp?hl=pt-PT>.

^{ix} Tiny Eye. Disponível em <https://www.tineye.com/>.

^x Recomendo a leitura do artigo Exif Metadata: a investigação policial subsidiada por sua extração e análise, disponível em <http://direitoeti.com.br/artigos/exif-metadata-a-investigacao-policial-subsidiada-por-sua-extracao-e-analise/> onde podem ser extraídas informações e fontes de consulta de metadados de fotografias.

^{xi} Foto Forensics – disponível em <https://fotoforensics.com/>, permite através da função ELA – Análise de Nível de Erro-, identificar as áreas que estão dentro de uma mesma imagem com níveis de compressão distintos. Pode ser bastante útil para tentar demonstrar montagens numa fotografia.

^{xii} Disponível em <https://www.google.com.br/alerts>.

^{xiii} O serviço encontra-se acessível no link <https://www.talkwalker.com/alerts> que permite a criação de alerta para recebimento de resposta através de email previamente cadastrado.

^{xiv} Outras ferramentas para buscas podem ser encontradas na obra Investigação Digital em Fontes Abertas, da Editora Brasport.

^{xv} Disponível em <https://hoaxy.iuni.iu.edu/>.

^{xvi} Disponível em <http://hashtagify.me/>.

^{xvii} <https://www.hashtags.org/analytics/fy/>.

^{xviii} Disponível em <https://tweetdeck.twitter.com>

^{xix} O site <https://www.trendsmap.com/> permite georeferenciar as últimas tendências do Twitter. No mesmo sentido o site <https://onemilliontweetmap.com>.



^{xx} Disponível em <https://twitterfall.com/>.

^{xxi} <https://botometer.iuni.iu.edu/#/>.

^{xxii} <https://registro.br/cgi-bin/whois/>, <http://geektools.com/whois.php>, <https://www.arin.net/>,
<http://www.dnsstuff.com/>, <http://whois.domaintools.com/>, <https://who.is/>.