3. **DETECÇÃO DE FAKE NEWS**

A detecção de Fake News em si começa a ser abordada em 2015, e ainda não temos pesquisas sólidas que enriquecem o tema na academia. Oque vemos são várias tentativas e começos de artigos e que estão sendo feitos independentemente e apresentados em conferências e revistas. Apesar disso, desenvolveu-se uma certa estratégia, ou plano de pesquisa, ao redor do tema.

Neste capítulo falaremos justamente desse plano de pesquisa, que é dividido em três partes, a qual iremos abordar separadamente. Esse plano é, atualmente, a maior base para reconhecimento de padrões aplicados em detecção de Fake News divulgado. É essencial então que se entenda o processo por trás de cada etapa para que se possa compreender e possivelmente fazer um algoritmo visando a não propagação de Fake News.

As três fases dizem respeito a partes relativamente diferentes do processo, sendo a primeira sobre deteção de conteúdo em si, saber se uma notícia se caracteriza como uma notícia falsa como definimos anteriormente. A segunda fase diz respeito a detecção de fontes, que pode ser um trabalho grande por si só, pois deve-se buscar as referências da notícia e fazer a detecção de conteúdo nelas, enquanto checa-se a integridade de autores ou instituições e vê-se se há alguma forma de ganho pessoal ao divulgar aquela notícia. A terceira e última fase é a mudança de mentalidade nas pessoas, que trabalha o funcionamento de certas tecnologias como redes sociais, como isso afeta o psicológico das pessoas, fazendo-as divulgar mais Fake News, e maneiras de mudar isso.

3.1 DETECTANDO O CONTEÚDO

O problema da detecção de conteúdo é um dos maiores desafios da detecção de padrões aplicados em Fake News, pela falta de dados existentes. Qualquer conteúdo da Ciência de Dados é mais bem trabalhado com muitos dados. Com assuntos novos, como a detecção de Fake News, esse ramo tem certas problemáticas mais desafiadoras. Para resolver esse problema surgem iniciativas de aglomerar dados de Fake News, como a organização “Fake News Challenge”.

A ideia é dessas organizações é dar problemas reais com conjuntos de notícias, com algumas notícias falsas, como é no mundo real, e pessoas se unem para desenvolverem soluções que detectam quais dessas notícias são falsas e ver o quão preciso os algoritmos conseguem ser, além de debater pontos éticos no assunto.

O primeiro desafio é construir esses conjuntos de dados no qual ocorrerá testes e tentativas. Esse porém é um trabalho exaustivo e não muito apreciado pelos cientistas, apesar de ser extremamente importante, e deve ser feito de maneira cuidadosa para servir como um teste formal e verificar qualidade de futuros algoritmos [Van den Broeck J, Argeseanu Cunningham S, Eeckels R, Herbst K, 2005 ]. Abordaremos mais esse assunto na sua sub-secção própria.

A próxima parte é fazer algoritmos que rodem nesses conjuntos de dados e retornem com alguma precisão oque é uma notícia falsa. Esses algoritmos devem levar em conta, como já dito no capítulo anterior, nuâncias do que é uma Fake News, e isso dificulta bastante seu trabalho.

Como toda nova área da computação, os algoritmos estão sendo desenvolvidos de formas mais simples, e em nível de implementação, a definição de Fake News deve ser mais formal para que uma máquina processe-a. O interessante com o aprendizado de máquina, área pai da detecção de padrões, é que pode-se “treinar” um algoritmo, de forma que ele fica mais preciso quanto mais usado. Isso demonstra o porquê da falta de dados ser um problema, mas dessa forma, existem certos níveis de detecção desenvolvidos e treinados ao longo dos anos, que tem suas qualidades. Falaremos aqui dessa noção e de alguns desses algoritmos numa subseção posterior, numa ordem crescente de otimização, e consequentemente, temporal.

3.1.1 Construindo conjuntos de dados

A maior parte do tempo um cientista de dados não está analisando os dados em si, mas criando a plataforma para que os algoritmos rodem. Essa plataforma são os conjuntos de dados. É como construir um míssil super potente, o algoritmo, mas ele estar mirando na direção errada, ou a plataforma não aguentar o seu peso, ou ter feito todo o cálculo no planeta errado.

É essencialmente importante então fazer bons conjuntos de dados e para isso há uma série de passos para chegar o mais próximo possível de um conjunto óptimo, que minimize erros nas etapas seguintes. Essa série de passos envolve cinco processos, que serão falados a seguir.

É importante saber que há diversas outras preocupações quando tratamos de dados, saber se são qualitativos, quantitativos, possíveis atributos relevantes, se há erros, se é um conjunto válido para se analisar, e diversas outras questões. Isso também é uma questão de responsabilidade dos cientistas, tópico já abordado, pois dados mal utilizados podem acarretar em desinformação e gasto de recursos.

3.1.1.1 Limpagem de dados

O primeiro e mais importante passo da preparação de dados que lida com corrigir dados inconsistentes é preencher valores faltando e corrigindo dados “ruído”, que são valores incorretos ou de margem. Podem ter muitas células numa planilha, por exemplo, faltando dados, com inconsistência, valores duplicados, ou erros aleatórios. É nessa fase que possivelmente esses casos serão resolvidos.

Como eles são resolvidos vai depender dos requerimentos de projetos e irá variar, em geral, usa-se valores médios ou uma constante global para que ao usar fórmulas estatísticas, não mude drasticamente o resultado. Existem técnicas de reduzir ruídos de todo o tipo, que já não cabem no escopo desta monografia.

3.1.1.2 Integração

Essa etapa busca resolver erros de integração ao juntar vários esquemas, conflitos que podem ser gerados a partir de redundâncias ao juntar vários dados diferentes. Basicamente, aplica-se outra limpeza nos dados agora integrados.

3.1.1.3 Transformação

Aqui, pega-se os dados, que podem ser gigantes, e usam-se alguns algoritmos de transformação, dependendo da aplicação: Normalização, generalização, agregação e muitos outros existem.

3.1.1.4 Redução

Uma fazenda de dados, como são chamadas grandes depósitos de dados, possuem Petabytes de dados e análises sempre rodando. Nesse passo a ideia é abstrair do conjunto de dados um universo onde todas as análises darão resultados parecidos, ou seja, um universo representativo. Existem diversas estratégias de redução de dados, baseado em diversos possíveis requerimentos ou tamanho do sistema.

3.1.1.5 Discretização

Os conjuntos de dados usualmente contém três tipo de atributos: contínuos, nominais e ordinais. Alguns algoritmos só trabalham bem com atributos categorizados discretos. Essa fase busca dividir intervalos contínuos em pequenos pontos discretos para que o algoritmos consiga rodar em futuras aplicações.

Sistemas de limpeza de dados são desenvolvidos há muito tempo, mas nos últimos anos eles vem tomando proporções maiores graças à importância de certos tópicos que a Ciência de Dados vem abordando, como o Fake News, e assim, ainda é uma área de muitas pesquisas. Empresas como a Google vem investindo bastante nessa área, com o *GoogleRefine*, tentando automatizar o processo da limpeza de dados. A *IDC FutureScape* prediz que o custo com manutenção e preparação de dados irá crescer duas vezes mais que o custo com desenvolvimento de fato.

Porém, essa automação não é fácil de fazer, visto que a preparação de dados é mais visto como uma arte, que muda de aplicação em aplicação, e é necessário que os cientistas tenham a responsabilidade de saber lidar com essa parte do processo. Todo dado não limpo é dado sujo, e numa aplicação real e minuciosa como a detecção de Fake News, é extremamente necessário que esse processo seja bem feito.

3.1.2 Algoritmos de *Flag*

São chamados algoritmos de *Flag* aqueles que a partir de um input de várias pessoas que avisam que aquele conteúdo parece ser falso, ele é analisado separadamente e detectado se é Fake News ou não. Essa solução é bem simples, e foi uma das primeiras a surgir principalmente em redes sociais. O Facebook, por exemplo, lançou em 2017 uma forma dos usuários reportarem oque era Fake News na plataforma.

A ideia desses algoritmos é similar, apesar de haver algumas diferenças que serão abordados aqui, é que o agregado dos sinais dos usuários pode ser usado como um identificador de uma potencial Fake News. Essa notícia pode então ser mandada para um expert para revisar rapidamente. Se confirmada falsa, deverá ser tirada do sistema ou marcada para não aparecer em foco e não ser muito divulgada.

Existe porém uma segunda fase depois dos *flags* para filtrar as notícias que serão mandadas para o expert, de maneira que não haja má intenção de usuários para quebrar o algoritmo. Essa segunda fase está sendo explorada em pesquisas recentes, iremos descrever nesta monografia a abordagem padrão e um algoritmo específico.

Os métodos computacionais para detecção de Fake News, em geral, usam de grande parte de algoritmos de detecção de rumores e avaliação de credibilidade que já existiam. Esses métodos são tipicamente baseados em modelos preditivos para classificar se uma notícia é falsa. Numa abordagem padrão, isso é feito com os seguintes métodos: (i) Baseado em análises via processamento de linguagem natural; (ii) Via treinamento de modelos de detecção de fontes e confiança; (iii) Análise do sistema e arredores de onde a notícia é encontrada; (iv) Uma combinação desses fatores citados.

Existem porém, como já citado, diversos problemas cruciais na detecção de Fake News, subjetividade no tema, limite de dados, uma grande gama de possíveis compartilhadores(pessoas que não sabiam que era Fake News). Em suma, os métodos computacionais sozinhos atualmente não conseguem abordar o problema de maneira suficientemente boa.

Surge então a ideia dos sinais de pessoas para direcionar a detecção para apenas certas notícias. Esse método já foi usado antes para aplicações diferentes de segurança *web*, e já existiam estudos que mostravam uma variação grande na performance desse tipo de algoritmo dependendo do público daquela plataforma. Em redes sociais a possibilidade de fraude por votos de pessoas é alta[Mandell, 2017].

A forma então com maior índice de acertos na detecção é a junção de sinais de pessoas, algoritmos de avaliação e a validação com expert, abordagem essa que pode ser vista como uma semi supervisionada, procura minimizar as fraudes do usuário com o expert e filtrar o número de notícias que chega e ele via algoritmos.

3.1.2 Algoritmos óbvios

Algoritmos óbvios focam em pegar apenas oque é mais obviamente Fake News, eles concentram sua atividade no grupo de notícias mais problemáticas mas também com a linguagem apelativa mais característica e títulos alarmantes, deixando fácil sua detecção. Apenas atingir esses tipos de notícia já é um grande avanço, principalmente como um algoritmo inicial. Com isso em mente, tenta-se detectar as Fake News mais simples possível, assim não precisando de importar com toda a área nebulosa de erros, sátiras e verdades pessoais.

Uma das formas de fazer isso é ver se o título da reportagem bate com o corpo do texto, apenas de fazer isso já há um grande corte na divulgação de notícias falsas.

Outra maneira é procurar por palavras alarmantes, como ‘final”, “último”, “nunca”, nomes de pessoas famosas junto de adjetivos como “maior”, “melhor”, e analisar separadamente essas notícias.

Algoritmos desse tipo são uma grande ajuda de vanguarda, pois analisam a partir dos erros e notícias que não são detectadas alguns detalhes antes não vistos pelos cientistas. Existem diversas técnicas para fazer isso e muitas delas já estão em bibliotecas para linguagens de aprendizado de máquina como R e Python, onde qualquer um pode contribuir e fazer seu próprio sistema de detecção de Fake News. Isso é também relevante, pois com ajuda de mais programadores é possível encontrar mais soluções para o problema.

3.1.3 Algoritmos wikipedia hoaxes

A fundação Wikipedia começou, pouco depois de seu surgimento, a iniciativa “Wikipedia Hoaxes”, que visava achar erros em artigos escritos na plataforma e documentá-los. Tudo era com ajuda dos próprios usuários do sistema, mas ao longo dos anos, isso foi se tornando uma grande fonte de dados e começou-se a reconhecer padrões em artigos que eram futuramente descobertos como Hoaxes, fazendo com que os usuários reconhecessem antes os erros.

Essa interação entre usuários ao longo dos anos levou a algoritmos informais, mais como heurísticas, de como suspeitar que um artigo escrito estava errado. Como a desinformação na Wikipedia veio muito antes do reconhecimento de padrões ser usado para detectar Fake News [Kumar; West; Leskovec (2016)], o sistema de dados da mesma tem muito mais informação que os cientistas.

Esse banco de dados serviu de inspiração para diversos algoritmos aplicadas na área hoje. e se baseia em certos parâmetros, desenvolvidos na prática ao longo dos anos em que a Wikipedia Hoaxes foi se formando: (i) Aparência, seria como a notícia foi escrita, tipo de linguagem, qual o tamanho do texto, proporção entre texto e imagens, quantidades de links para a própria wiki, e quantidades de links externos; (ii) Rede de links, é como aquele artigo se relaciona com outros pŕoximos, e para isso usa-se teoria dos grafos para inferir coerência no artigo; (iii) Suporte, quando aquele artigo foi linkado pela primeira vez, e quem linkou-o; (iv) Criação, quem criou o artigo e qual a experiência dele criando ou editando artigos da Wikipedia.

Baseado nesses parâmetros foi observado ao longo dos anos que os Hoaxes tinham menos proporção entre fontes e texto, artigos linkados tinham edições do mesmo endereço IP do criador do artigo, que tinham edições apenas recentes. Assim, foi criado a partir dessa heurística, um detector de Hoaxes na wikipedia que era melhor que as tentativas anteriores.

A ideia foi então se basear nesse algoritmo para fazer um de detecção de Fake News, considerando as devidas mudanças que nem tudo será da Wikipedia, mas mesmo assim, está sendo possível fazer grandes avançados baseados nisso.

3.2 DETECTANDO A FONTE

Detectar a fonte de uma notícia é também um ponto importante pois pode facilitar o trabalho da delimitação de escopo, se a fonte da notícia for um site de sátiras, por exemplo. A ideia é descobrir se a fonte é humana, tweetando ou compartilhando algo, ou bots e sites, que estão gerando dinheiro com propagandas. Descobrir isso permite aos cientistas trabalharem com diferentes aspectos do problema.

As pesquisas nesse ramo ainda são muito recentes, e assim como na detecção de conteúdo, buscaram trabalhar em cima de algo já estabelecido. O foco então passou a ser na detecção de Bots, pois já existiam diversos sistemas que detectam-os, e apenas tirando os bots já é possível diminuir bastante a divulgação em larga escala de Fake News, que não é o objetivo final mas é um bom meio de se chegar nele.

Bots são sistemas autônomos que compartilham notícias ou escrevem e usam redes sociais por meio de um script, então não há realmente ninguém por traś da máquina. Os Bots podem ser feitos por diversas razões, por exemplo, você pode fazer um bot no twitter que todo dia de meio dia tweeta a meteorologia do tempo de hoje em Recife, por outro lado, pessoas fazem Bots para se aproveitar de sua velocidade para compartilhar em massa informações que seriam tiradas do ar rapidamente, ou para outros fins maliciosos, como esconder quem está por traś do compartilhamento.

A ideia é usar sistemas de detecção de Bots já estabelecidos e trabalhar em cima deles para adaptá-los à Fake News. Serão abordados nessa pesquisa dois desses sistemas, pois é interessante observar qual as abordagens para detecção desses scripts, pois eles fazem um paralelo com a detecção das Fake News muito interessante.

Os Bots podem ser categorizados pois sua ação, por mais semelhante que o programador que fez o script quis que parecesse com o humano, ainda tem certas falhas. Os sistemas abusam dessas falhas de diferentes formas para detectar-los, iremos analisar justamente qual a forma que os sistemas usam e seus parâmetros para isso[ [Varol](https://arxiv.org/search?searchtype=author&query=Varol%2C+O), [Ferrara](https://arxiv.org/search?searchtype=author&query=Ferrara%2C+E), Davis, [Menczer](https://arxiv.org/search?searchtype=author&query=Menczer%2C+F), [Flammini](https://arxiv.org/search?searchtype=author&query=Flammini%2C+A), 2017].

3.2.1 BotOrNot

A ideia inicial do BotOrNot era melhorar a plataforma Twitter, fazendo com que pessoas conversem com pessoas, uma interação muito mais agradável, e não com Bots. Eles avisam para os usuários se eles tinham seguidores que eram bots, ou se a pessoa que ele estava conversando tinha seguidores que eram bots. Hoje em dia a ideia é mais para divulgação de perfis de maneira mais centrada em humanos, que é mais eficiente.

O importante é analisar que tipo de ferramentas ou parâmetros ele ao longo dos anos desenvolveram para detectar os bots, e tentar usá-las para detectar especificamente bots de Fake News. Tais ferramentas são: (i) Usuário, analisar a foto de usuário, data de criação da conta, e em geral todas as features de usuário; (ii) Amigos, a mesma análise mas para os amigos mais próximos ou mais distantes; (iii) *Network*, quão densa é a rede de amigos, quantos amigos *retweetam* ou visualizam os tweets, qualquer ação que envolva seguidores; (iv) Temporal, quão frequentemente a conta tem atividade, se é no mesmo período do dia, intervalo entre tweets; (v) Linguagem e conteúdo, se a conta tweeta em várias línguas, sobre sempre a mesma coisa, se faz sentido; (vi) Sentimento, Bots tem um padrão de expressar possíveis sentimentos muito diferente de humanos[ Dunham, Ken; Melnick, Jim (2008)].

Essas características não parecem muito diferentes das exploradas na seção anterior, e realmente não são. Baseado nelas, o BotOrNot consegue inferir uma porcentagem de chance de qualquer conta do twitter ser um bot. Apesar de limitado para essa rede social, aplicações como essa são de extrema importância, por já conter alguns anos de trabalho de base sobre temas parecidos com a detecção de Fake News, e por tem grandes conjuntos de dados em que os cientistas podem trabalhar para testar os algoritmos.

3.2.2 Lei de Benford

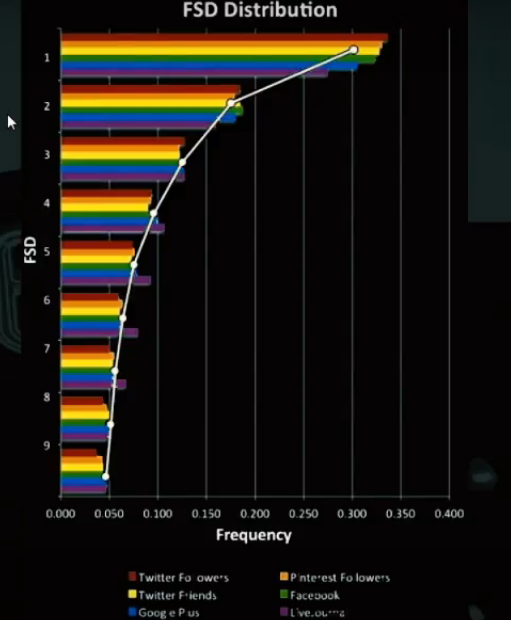
A lei de Benford não é necessariamente um sistema, mas é de muita importância pois muitos dos melhores sistemas de detecção de Bots e desenvolvimentos na área de Fake News estão levando em conta essa lei para seus algoritmos. Ela é uma observação da distribuição de frequência nos primeiros dígitos de muitos conjuntos de dados da vida real. A lei diz que em ocorrências de conjuntos numéricos, o primeiro dígito tem uma tendência muito maior a ser pequeno. O número um por exemplo, aparece 30% das vezes, enquanto 9 apenas 5%. Com essa informação, a lei faz predições dos próximos dígitos, combinação de dígitos, e muitas manipulações com esses números em geral. Essa lei é tão poderosa que pode ser usada como prova de fraudes bancárias[Weisstein, Eric W. 2015].

Vários sistemas então usam dessa lei para agregar dados e analisar separadamente pontos que desviam de tal fenômeno. A ideia é ver a quantidade de seguidores que uma conta tem, e seus amigos, em diferentes redes sociais, e analisar a porcentagem de amigos que um número de seguidores que começam com um, e esse número deve ser muito maior do que com o número oito ou nove, por exemplo. De fato essa distribuição segue a lei de Benford, e a partir dela é possível observar anomalias em certas contas[Goldbeck, 2015].

Um estudo feito especificamente no Twitter, com contas aleatórias, fez o ranking com os seguidores e ordenou as contas de acordou com o quanto seguiam a lei de Benford. O resultado foi que as 250 contas mais abaixo eram todas de Bots ou Fakes, que compartilhavam, dentre outras coisas, informações falsas. O interessante é que essas contas não tinham muitas das características descritas nas seção anterior, ou seja, não eram detectadas pelo algoritmo do BotsOrNot e de muitos outros sistemas[Goldbeck, -].

Sistemas de detecção de Fake News estão tentando então implementar esses padrões, mas como discutido em seções anteriores, faltam dados para treinar os algoritmos, e por ser um tema muito recente, pesquisas ainda estão sendo desenvolvidas para formar heurísticas ou algoritmos mais formais.

Detectando que uma notícia provém de bots, e não de pessoas físicas, é de suma importância para a detecção das Fake News, filtrando dessa forma podemos aplicar algoritmos apenas em um subconjunto das notícias, eliminando possibilidade de erros. O problema é que as pessoas também são responsáveis muitas vezes pela divulgação de uma notícia falsa. Quem inicia é um bot, mas as pessoas espalham essa notícia muito rapidamente, e quando for detectado que era a notícia de um bot, elá já está compartilhada em toda a rede. Falaremos sobre mais problemas com a detecção da fonte na parte final da monografia, desafios e o futuro, e na próxima subsecção sobre a mentalidade dos usuários de redes sociais, que impacta muito na propagação das Fake News.



3.3 MODIFICANDO INCENTIVOS

A maior fonte de compartilhamento de Fake News ainda são as pessoas em si. Por causa da linguagem, que até usamos para detectar-las, é muito mais chamativo uma notícia falsa do que a chata verdade. O último passo na detecção de Fake News diz respeito à modificar os incentivos que as fontes desse tipo de conteúdo tem para divulgá-lo. Para isso faz-se uma divisão das fontes, já faladas na seção anterior, em dois principais focos, pessoas e sites, que são observados a partir de possíveis incentivos para compartilhar conteúdo falso. A partir disso são desenvolvidos certas estratégias e pode-se definir exatamente para que tipo de público aquela estratégia funciona.

As pessoas então estão divididas em: (i) Se importam com o conteúdo compartilhado ser Fake News; (ii) Não se importam se o conteúdo compartilhado é Fake News. O primeiro se avisado que certa notícia é falsa, não irá compartilhar, e possivelmente avisará a pessoas a veracidade daquilo quando questionado. O segundo grupo, porém, é o mais complicado, se avisado que algo é Fake News, ele não vai se importar e vai continuar a compartilhar. O incentivo desse grupo é curtidas ou propaganda pessoal,

Os sites estão divididos em: (i) Querem ganhar dinheiro com os cliques a partir da divulgação de Fake News; (ii) Querem gerar algum tipo de propaganda com as notícias falsas, como na eleição presidencial dos Estados Unidos de 2016. Os incentivos desses grupos são mais simples, sendo mais fácil modificá-los, pois eles dependem fortemente da plataforma de divulgação das notícias.

A questão é aplicar a modificação de incentivos específica para cada um desses grupos, pois eles são muito diferentes. Algumas estratégias, porém, funcionam para mais de um por ser mais generalizada, porém, a dificuldade de implementação das mesmas é maior e mais dependente de terceiros, como a maneira de redes sociais divulgam conteúdo. Abordaremos então maneiras efetivas de modificar esses incentivos para cada grupo nas próximas subseções.

3.3.1 Bloqueio de Ads

O incentivo do ganho de dinheiro é simples de se combater, uma vez cortado a possibilidade de um site ganhar dinheiro a partir da divulgação de Fake News, ele não terá mais esse incentivo para compartilhá-la. Há algumas maneiras de se fazer isso, sendo a mais óbvia a plataforma de divulgação retirar monetização de qualquer página ou site que compartilhe notícias falsas. Isso, como já dito, é uma forma genérica de resolver e assim depende que redes sociais sejam ativas no processo e percam parte do dinheiro que iria para eles.

Outra forma é de não divulgar posts de páginas que propagam Fake News, ou divulgar de forma menos pejorativa. Não deixar outras pessoas compartilharem, ou não entregar para um grande número de pessoas seriam duas maneiras mais específicas de fazer isso. Assim, o incentivo que seria ganhar dinheiro seria menor, pois os sites ganham bem menos dinheiro por essa notícia.

3.3.2 Aviso para usuários

Para usuários que se importam com o fato que estão compartilhando Fake News, mas muitas vezes não sabem e compartilham, basta ter avisos prévios, para que ele saiba que oque está compartilhando não foi embasado por certas instituições ou por algoritmos de detecção.

O Facebook recentemente começou a fazer esse tipo de abordagem,



avisando para usuários antes deles compartilharem, que aquela notícia tem altas chances de ser falsa. Esse tipo de iniciativa já melhorou a plataforma e faz com que esses usuários ainda percebam a quantidade de mentiras que compartilham e lembrem dos sites que estão fazendo esse tipo de coisa.

Isso não funciona, porém, para pessoas da categoria que não se importam que é Fake News, e na verdade, tem um efeito inverso. Essas pessoas acham que essa mensagem é uma tentativa da mídia de silenciá-los e acaba compartilhando mais vezes.

3.3.3 Forma de compartilhamento

Atualmente ao compartilhar um link nas maiorias das redes sociais, você estará compartilhando uma miniatura em imagem, um link clicável, um título que foi escolhido pelo site, e o nome do site. Isso é bastante informação, e é útil em diversas situações pela facilidade que outros usuários têm de acessar o link que possivelmente seu amigo na rede social compartilhou. O problema vem quando esse compartilhamento for de uma Fake News. A forma que isso é feito dá muita propaganda para a notícia e para o site que compartilhou, e facilita que amigos só leiam a manchete, a apertem o botão de compartilhar também.

Cientistas de dados promovem que o compartilhamento de notícias que tem grandes chances de serem Fake News se dê apenas com o link, não clicável, sem miniatura ou título do artigo. Dessa forma, é possível mudar o incentivo da propaganda que é feito, e principalmente em épocas mais propícias a terem Fake News, essa medida poderia ser aplicada mais rigorosamente.

Fake News são divulgadas muito mais que notícias normais, isso se dá pela psicologia humana, e sites que sabem que pessoas divulgam mais notícias com uma linguagem mais chamativas. Em 2016, uma notícia do papa apoiar a candidatura de Donald Trump foi compartilhada mais de um milhão de vezes, e era falsa. A notícia verdadeira foi compartilhada apenas 33 mil vezes no Facebook. Apesar disso ser bom para algoritmos detectarem, pois entram em diversos pontos citados anteriormente nessa monografia, faz com que os mesmos sites abusem de certos padrões psicológicos, como a da mentira sendo compartilhada muitas vezes, que comprovadamente tem um impacto nas pessoas que faz com que elas comecem a acreditar na mentira, para que quando detecta-se que é Fake News, a notícia já tenha se espalhado por toda a rede social.

Sites como Facebook tem muitos dos recursos que os cientistas não tem, como enormes conjuntos de dados e recursos. Eles poderiam botar em prática vários dos algoritmos que os cientistas idealizam mas ainda não podem implementar. Esses tipos de parceria também são ideais para o combate à Fake News.

3.4 Considerações do capítulo

Neste capítulo foi discutido um pouco sobre a estratégia atual mais proeminente na detecção de Fake News, que é dividida em três passos. Apresentamos algoritmos e heurísticas das três partes, começando pela detecção do conteúdo da notícia ser falso, que é dividido em uma preparação para que o algoritmos rodem, que chamamos de limpagem de dados, e depois foi apresentado alguns algoritmos mais populares e os incentivos por trás deles, foram esses os algoritmos de *flag*, os algoritmos óbvios e as Wikipedia Hoaxes. Depois disso foi apresentado as estratégias de detecção de fonte, a qual o foco foi nos Bots, sistemas de script usados por sites para compartilhar notícias ou fazer uma rede de conexão de amigos em redes sociais para divulgar notícias. Foi mostrada a Lei de Benford e como ela impacta nos dados mundiais e pode ser usada como um auxiliador para mostrar anormalidades em redes sociais e detectar possíveis fraudes de usuários, ajudando na detecção de Fake News. Por fim abordamos a modificação dos incentivos que as pessoas ou sites tem ao compartilhar o conteúdo falso. Dividimos os grupos a partir de certos parâmetros e para cada tipo de fonte vimos uma abordagem diferente, algumas que já estão sendo aplicadas, como o aviso prévio para pessoas, ou outras idealistas que só poderiam ser testadas com ajuda de grandes redes sociais como o Facebook.