UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

GUILHERME GOUVEIA FIGUEIREDO LIMA
MARINA OLIVEIRA DE BARROS

CIÊNCIA DE DADOS E FAKE NEWS:
Histórico, Técnicas e Desafios

RECIFE
2018
UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

GUILHERME GOUVEIA FIGUEIREDO LIMA
MARINA OLIVEIRA DE BARROS

CIÊNCIA DE DADOS E FAKE NEWS:
Histórico, Técnicas e Desafios

Monografia apresentada como requisito para aprovação na matéria de Metodologia e Expressão Técnico-Científica (IF676) no curso de Ciência da Computação, Centro de Informática (Cin) da Universidade Federal de Pernambuco (UFPE).

Orientador(a):
Patrícia Cabral de Azevedo Restelli Tedesco

RECIFE
2018

RESUMO

"Fake News" é um termo que diz respeito a propagação de notícias falsas, seja para difamação ou até por pessoas que não sabem que se trata de uma mentira, e é tão preocupante que países estão fazendo leis contra ela. A ciência de dados é uma área da computação que estuda manipulação e organização de dados. Graças à imensa onda de Fake News dos último anos, vêm-se estudando como a ciência de dados está sendo usada para combater a ampla de divulgação dessas notícias, e para identificá-las. Essa pesquisa busca abordar a relação desses dois conceitos ao longo dos anos, que técnicas da ciência de dados são usadas em cada etapa do desafio que é a censura de Fake News e quais tendências podem surgir acerca dessa relação.afinal, na grande maioria, os documentos são textos livres, com dados não estruturados ou semiestruturados.

Palavras chave: Notícias, dados, manipulação, técnicas, censura, divulgação.

SUMÁRIO

1. INTRODUÇÃO

Desde os primórdios da humanidade, em épocas como as da monarquia, a divulgação de informação falsa é usada para algum pretexto de ganho pessoal. Seja difamação sobre algum adversário ou apenas por ganho material. A limitação da informação sempre foi um problema, porém, para que esse tipo de prática fosse detectada ou questionado pela população. Era impossível, na idade das trevas, por exemplo, quando a informação era monopolizada por instituições religiosas, de saber quais eram as notícias falsas. Durante muitos séculos seguintes, a mídia era quem controlava e monopolizava a divulgação da informação e usava isso como uma massa de manobra.

Surge então com a era moderna a computação, e com ela a resolução de vários problemas que agora com processamento computacional são mais facilmente abordados. Um dos campos, a Ciência de Dados, consegue por meio de processamento e manipulação de dados, dentre muitas outras coisas, encontrar padrões, tendo assim um novo meio de resolver o problema da divulgação de informações mentirosas, fenômeno que chamamos hoje de Fake News.

Esse tema ainda vem sendo mais destrutivo nos dias de hoje, pois com a facilidade da informação vem também a facilidade de divulgá-la, um bom exemplo é a eleição de 2016 dos Estados Unidos, onde parte da campanha dos concorrentes era difamar os outros candidatos com notícias falsas, que até hoje, depois do presidente Trump ter sido eleito, vem à tona. O termo Fake News em si foi popularizado pelo próprio presidente.

Os pesquisadores da Ciência de Dados vem tendo então um interesse maior nos últimos anos na questão da detecção dessas notícias falsas, fazendo diversas estratégias e formulando um método para que pessoas possam trabalhar em cima e desenvolver formas próprias de detecção. O ponto disso é que há de ser um trabalho descentralizado, pois do mesmo jeito que a informação é difundida de forma mais rápida, a Fake News se espalha também mais rapidamente.

Esse trabalho então tem o objetivo de explicar o método de detecção de Fake News pesquisado e porque ele foi feito assim, dar um contexto para a importância do tema, e introduzir certas noções gerais que ajudarão no entendimento desta área.

Essa monografia possui três capítulos principais, começando no próximo, onde é introduzido um histórico entre Fake News e a Ciência de Dados, que introduz ambos os conceitos e destrincha um pouco mais a definição do termo Fake News para os cientistas, que pode ser bastante complicada e dependendo dela, mudar sua forma de detecção. No terceiro capítulo é apresentado o sistema em três fases do combate à Fake News com a Ciência de Dados, explicando em detalhes o processo e o porquê de cada fase ser importante. No capítulo 4, é discutido o futuro da área, e desafios que ela enfrenta. Por fim, a monografia é finalizada com as conclusões deste trabalho.

2. CIÊNCIA DE DADOS E FAKE NEWS

A relação entre estes dois tópicos tem uma história recente, em se tratando da Ciência de Dados computacional, mas o fato da manipulação de dados ser usada em notícias é algo muito antigo [McLachlan, 2017]. Porém, desde 2010, esse vem sendo um tópico de crescimento na indústria da computação, ao mesmo tempo que há uma crise de Fake News em vários países, virando tópico de leis nacionais na Europa, por exemplo. Os cientistas então viram oportunidades de como usar técnicas tanto para divulgação quanto para detecção de Fake News, surgindo um novo campo de pesquisa na área, o qual vem sendo extremamente importante e requisitado. O que a Ciência de Dados faz é usar de dados, hoje abundantes no mundo tecnológico, para melhorar relação com clientes, fazer propagandas direcionadas ou detectar fraudes, tudo isso analisando padrões [Provost, Fawcett, 2013]. A razão disso impactar na detecção de Fake News é que, assim como um email *spam*, há padrões para notícias querem chamar atenção, padrões esses que vêm da percepção humana[Van der Linden, 2017]. A Ciência de Dados porém vai além disso, podendo ser usada de maneira a mudar a percepção das pessoas, e fazer com que as notícias falsas não sejam apenas detectadas, mas parem de ser amplamente divulgadas.

Neste capítulo o que abordaremos é um histórico da relação entre esses dois temas e daremos uma definição mais formal para Fake News, a qual será usada no capítulo 3, e uma secção sobre os cientistas de dados em si e suas responsabilidades ao trabalhar com esse assunto.

2.1. HISTÓRIA

Não podemos falar da relação entre os dois tópicos sem citar o ano de 1948, quando o jornal Chicago Daily Tribune imprime a icônica frase “Dewey defeats Truman”, quando na verdade o contrário havia acontecido. Isso foi um grande impacto na época, porém o fato foi usado como uma sátira pelo próprio Truman, que ridicularizou o adversário, gerando uma famosa foto dele segurando o jornal(Figura 1).

A repercussão disso levou os jornais a notarem como notícias como essa davam vendas. Na tirinha “The Evil Spirits of the Modern Day Press”[1888](figura 2), já vemos sátiras de como a mídia controlava a população a partir de manchetes enganosas. Nessa época, porém, pouco a população podia fazer. A verdade é que Fake News, representando histórias enganosas amplamente divulgadas, data de muito antes, até em épocas medievais ou antes de Cristo [Weir William ,2009]. Histórias como o Cavalo de Troia, que não sabemos até a hoje da veracidade, são exemplos disso.

Figura 1 - Truman levanta o Chicago Daily Tribune com a manchete errada

Fonte: Wikimedia Commons

Figura 2 - The Evil Spirits of the Modern Day Press[1888]

Fonte: Wikimedia Commons

Por outro lado, os estudos de Ciência de Dados começaram muito tempo depois, por volta de 1960, mais tarde, numa conferência, o nome foi usado com seu significado atual pela primeira vez[Press Gil, 1996]. Antes disso, era mais um sinônimo de Ciência da Computação

em si. Por enquanto era visto como um ramo da estatística computacional que trabalhava com dados.

Foram nos anos 2000 que estudos mais focados começaram a se desenvolver, com um estudo em particular no qual o autor visava marcar e expandir as áreas da chamada Ciência de Dados[Cleveland, W. S. 2001], isso desencadeou uma série de pesquisas que aprofundaram várias temáticas e trouxe elas para o campo da mesma, dentre essas, o principal método de combate à Fake News, o reconhecimento de padrões.

A área de reconhecimento de padrões já era estudada antes, em áreas como Psicologia. Mas foi modificada levemente e entrou, junto com o aprendizado de máquina, no ramo da Ciência de Dados por volta dos anos 2000. Essas duas áreas têm muito em comum e é difícil delimitar começos e fins pelo menos com o histórico que temos hoje [Bishop Christopher, 2006]. Ambos os campos se baseiam fortemente na teoria matemática, porém, nesse estudo mostraremos apenas uma usagem prática do reconhecimento de padrões, logo, não irá se aprofundar neste tópico.

Estudos na área de reconhecimento de padrões, até então um ramo de estatística, e ainda não levava esse nome, foram se desenvolvendo desde 1960, quando eram puramente matemáticos, e não havia prospecção de uma utilidade prática nela, menos ainda como uma solução para Fake News. Os estudos rodavam em torno de resolução de problemas matemáticos, apesar de já existir princípios que levariam esse conceito para a computação, como abstração de grandes quantidades de dados e análises de informações complexas [V.N. Vapnik, A.Ya. Chervonenkis, 1974].

Perto da década de 80, surgem alguns estudos sobre a área de computação especificamente, no começo ainda com outro nome, mas agora visando o uso do processamento de computadores para resolver os problemas antes matemáticos. O reconhecimento de padrões não era ainda uma área por si só dentro da estatística, mas os tópicos falados são, hoje, do ramo do aprendizado de máquina. Na época, a *IEEE Transactions on Computers* teve diversos artigos publicados sobre esse tema. Era a febre da computação atingindo a estatística e era uma questão de tempo até as pesquisas ficarem mais concretas.

Nos anos 2000, junto com a já citada publicação de Cleveland, surgiram diversos estudos sobre aplicações mais reais do reconhecimento de padrões, agora com algoritmos que já abriam o campo para ainda mais pesquisas[Mineichi Kudo, Jack Sklansky 2000].

Nos próximos anos houve um aumento em tudo relacionado a Ciência de Dados, a descoberta constante de novos e melhores algoritmos levavam a técnicas da estatística a serem usadas em novos campos, empresas lucraram muito com a mineração de dados. Ao longo dos anos, isso só foi aumentando. Em 2011 houve um aumento de 15,000% em trabalhos procurando por Cientistas de Dados, seminários e conferências sobre o tema tomaram conta de convenções de computação[Keith D. Foote, 2016].

Foi durante esse tempo que a aplicação de detecção de padrões começou a ser usada para problemas reais, a detecção de Fake News viria a ser uma dessas aplicações.

Nessa época, o Facebook começava a crescer, e a Ciência de Dados, especificamente o reconhecimento de padrões, começou a ser usada com uma aplicação de manipulação, para mostrar à pessoas o que elas querem ver. Esse tipo de uso se transformaria na grande crise de Fake News, a qual ocorreu entre os anos de 2015 e 2017 na eleição presidencial Norte

Americana, que fez com que notícias falsas fossem amplamente divulgadas, e mostrou o quanto isso funcionava como massa de manobra. A partir desse evento, portais de notícia seguiram a tendência. Se preocupar se uma notícia é verdadeira antes de compartilhá-la virou uma preocupação global.

Surgem então, a partir de 2016, pesquisas ,dentro da área do reconhecimento de padrões, relacionadas à Fake News. Por ser recente, ainda não há estudos muito aprofundados, porém já se tornou o maior desafio dessa área nos último anos, sendo extremamente destacada em conferências de Ciência de Dados. Os estudos ainda estão sendo desenvolvidos e vemos nessas conferências as versões ainda em construção sendo apresentadas por cientistas mas não há ainda referências de fato de trabalhos englobando esse meio específico em 2018, sendo que há artigos sobre temas paralelos usados como base para essas pesquisas que serão apresentados ao longo desta monografia.

2.2. FATOS E VERDADES

A definição da palavra Fake News é extremamente importante para a Ciência de Dados resolver tal problema, e consequentemente, para essa pesquisa. A preocupação dos pesquisadores é que ao tentar censurar-las, eles acabem também censurando outros tipos de informação. Isso levou-os a um extenso debate moral e ético sobre onde os cientistas devem atuar.

A maior questão é diferenciar as notícias falsas e manipuladoras de duas coisas: erros e sátiras. O já citado exemplo de “Dewey Defeats Truman”, por exemplo, apesar de ser uma notícia falsa, não era Fake News da maneira que queremos detectar, já que foi um erro de impressão. Uma sátira em alguma tirinha ou site de notícias engraçadas poderia também divulgar algo como “Trump aponta *Alien* como possível ministro da economia”, que seria uma mentira, mas também não seria Fake News.

O desafio é então definir o que exatamente é que deve ser procurado por algoritmos de reconhecimento de padrões para detectar Fake News. A ideia é que apenas as notícias maliciosas, divulgadas com a intenção de enganar pessoas, sejam alvos da censura. Enganar é uma palavra essencial aqui, pois se alguém acredita em algo que a ciência prova o contrário, por exemplo, e divulga, não significa que essa pessoa está tentando enganar ninguém. Do ponto de vista dela, ela está apenas divulgando a verdade. Isso nos leva a ainda outro debate.

É uma grande questão então para os cientistas, definir qual escopo do que estão trabalhando, essa também é uma questão ética que será abordada na próxima subseção. Vamos então definir e discutir os termos que serão utilizados neste trabalho.

2.2.1. Fatos

Serão dito fatos, tudo que for provado cientificamente. São coisas como evolução das espécies, teorias físicas, provas matemáticas e principalmente, eventos bem documentados. A

principal preocupação é a divulgação de dados que não são fatos, como fatos. Não é um problema a divulgação de teorias, desde que o intuito seja de informação.

2.2.2. Verdades

Verdades é o que não pode ser considerado um fato, ou até vai contra um fato, mas não tem a intenção de denegrir, como crenças, ou teorias da conspiração. O ponto é que algumas pessoas acreditam em coisas e quando compartilham-na, não é com a intenção de enganar ninguém, pelo contrário, ela está tentando convencer outros a verem seu ponto de vista.

2.2.3. Sátiras

Sátiras são notícias que não tem intenção de divulgar informações, e assim, não tem intenção de enganar ninguém, apenas dar algum teor cômico a algum evento ou fato, que pode ser enganador mas as pessoas sabem que se trata de uma piada.

2.2.4. Fake News

Iremos chamar nessa pesquisa, e é como é visto por grande parte dos pesquisadores na área, de Fake News, notícias que divulgarem algo que for de encontro com um fatos históricos, ou não for nem um fato nem uma verdade. Assim, eliminaremos a censura de opiniões e pontos de vista. As sátiras não serão consideradas notícias, e assim, não serão também Fake News.

Tais definições servem para definir melhor o escopo do problema, e é o primeiro passo quando cientistas vão embarcar nesse meio de usar o reconhecimento de padrões para detecção de Fake News. Porém elas não bastam, apesar de termos essas definições, a existência de todas essas nuances dificulta muito algoritmos de detecção. Falaremos mais disso no capítulo 3, e como resolver esses problemas. O quesito de erros será melhor abordado na secção seguinte, onde será descrita a responsabilidade dos cientistas de dados na detecção de Fake News.

2.3. RESPONSABILIDADE DOS CIENTISTAS

Cientistas são humanos, e assim como tal, podem cometer erros e ter seus próprios pontos de vista. Na ciência em si, isso é relevado pelo fato que é algo muito difuso e incerto. Se uma teoria for provada errada por qualquer outro pesquisador, haverá um debate acadêmico e a ela provavelmente não será aplicada em nenhuma ação real. A verdade é que muito já foi debatido sobre a falsificação de teorias ou métodos na ciência no passado [Lydia Patton, 2014], e apesar de ainda haver certo medo por parte da academia científica, o problema não é mais alarmante.

A Ciência de Dados passa por um problema similar, por ser muito nova, e ser uma aplicação prática, algumas de suas áreas sofre certo risco de cair em mãos erradas. O reconhecimento de padrões, e especificamente a detecção de Fake News é uma dessas áreas.

Por ser tratar de um assunto delicado, quando falamos a respeito da censura, a detecção deve ser feita de maneira completamente imparcial, dado alguns parâmetros, como as definições que demos na secção anterior. Porém definições podem ser mal interpretadas e cabe aos cientistas que vão trabalhar com os dados que não usem os algoritmos de forma a prejudicar alguém ou censurar alguma notícia.

Não cabe aos cientistas então, julgar o conteúdo da notícia, e sim, se ela se enquadra na definição feita por eles, do que é Fake News. Eles têm, porém, certa liberdade ao tratar de erros, citados na seção anterior. Apesar de não se tratarem especificamente de Fake News, a maioria dos algoritmos visa pelo menos alertar o leitor de que aquilo é um erro.

Então nesse meio, em que o escopo é extremamente sinuoso, e fazer algoritmos que consigam diferenciar entre uma notícia falsa e uma sátira, por exemplo, é extremamente difícil, é ainda mais importante que os cientistas que fazem esses algoritmos tenham noção de sua responsabilidade e tarefa na detecção de Fake News.

2.4. CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foi discutida a relação dos dois tópicos desta pesquisa, um histórico de como Fake News sempre esteve presente na humanidade e como estudos da área de reconhecimento de padrões foram se desenvolvendo ao longo dos anos até se tornar robusta o suficiente para detectar essas notícias falsas. Vimos diversas pesquisas no começo da área que foram importantes, como a publicação de Cleveland, e o grande aumento na área da Ciência de Dados que ocorreu nos anos 2000, citado em livros como “Data Science, the sexiest job in the 21st century”.

Além disso foi visto a definição mais formal de Fake News que é usada pelos cientistas, e por qual motivo é importante dar essa definição, como os algoritmos podem ser criteriosos e que é uma dificuldade para que os algoritmos de detecção não virem uma censura.

Por fim, foi abordado o lado dos cientistas e como eles devem ter responsabilidade na hora de pesquisar e aplicar algoritmos para que a definição de Fake News seja seguida à risca e a sua detecção não se tornar algo perigoso.

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 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 próximos, 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 AS FONTES

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, Ferrara, Davis, Menczer, Flammini, 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)].

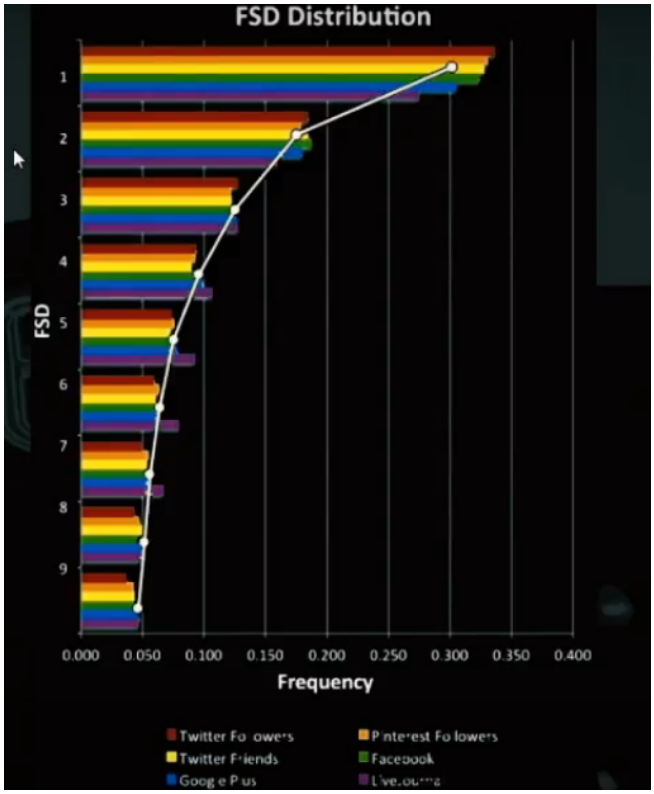
Essas características não parecem muito diferentes das exploradas na seção anterior, e realmente não são. Baseado nelas, o BotOrNot consegue inferir uma porcentagem de chance de qualquer conta do twitter ser um bot. Apesar de limitado para essa rede social, aplicações como essa são de extrema importância, 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](Figura 3).

Figura 3 - Distribuição em redes sociais mais famosas seguindo a lei de Benford



Fonte : Conferência Data Community DC

Um estudo feito especificamente no Twitter, com contas aleatórias, fez o ranking com os seguidores e ordenou as contas de acordo 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(Figura 4), 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.

Figura 4 - Facebook avisando que a notícia provavelmente é falsa

Fonte: Facebook

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 nesta 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.

4. TENDÊNCIAS E DESAFIOS

Depois das eleições de 2016 dos Estados Unidos terem passado, e as pessoas e instituições terem visto o impacto que Fake News podem ter, começou-se uma grande corrida de tecnologias para usarem dessa nova descoberta para algum fim. O foco desta monografia foi o fim da detecção de Fake News, e como toda nova tecnologia, há uma grande quantidade de desafios iniciais, prospectivas de problemas futuros, e possíveis tendências que essa área está tomando. Abordamos nos capítulo anteriores as estratégias e alguns problemas mas não necessariamente como eles se encaixam no contexto da Ciência de Dados, ou quais métodos estão realmente sendo mais usados.

Os grandes desafios atuais para essa área do reconhecimento de padrões aplicado na detecção de Fake News são: (i) As definições não muito claras sobre o que vai ser detectado, e como os cientistas podem entrar em desavenças por causa dessa definição, o que dificulta muito a manutenção de desenvolvimento de algoritmos; (ii) Falta de dados numerosos em que possam ser feitos testes, análises e treinamento de algoritmos, essenciais para a Ciência de Dados aplicar seus conceitos. Esses desafios iniciais levaram a certas estratégias citadas como pegar dados já existentes como sistemas de detecção de Bots, ou a Wikipedia Hoaxes.

Esses dois desafios não tem prospecção de melhora a não ser o tempo, que fará com

que o problema seja melhor analisado, aconteçam mais fenômenos como a eleição de 2016 e os cientistas entrem em consenso a partir dos estudos que estão sendo desenvolvidos mais ainda não terminados.

Enquanto isso há o desenvolvimento contínuo de sistemas, que a partir de falhas irão melhorando, e para isso há de se detectar quais os pontos mais relevantes na detecção de Fake News, analisando sistemas pré estabelecidos e a partir dos estudos que sairão nos próximos anos para construir modelos e heurísticas, e com isso ter-se uma análise numérica de quanto de fato esses algoritmos estão ajudando a prevenir a divulgação de Fake News.

Por fim, identificar intervenções que podem ser feitas em redes sociais, o principal ponto de propagação dessas notícias, e abordar as empresas para aplicarem essas intervenções, mostrando dados que comprovem a qualidade e transpareçam a iniciativa não como um apelo à censura mas como um meio de que as pessoas não sejam enganadas.

Como toda ciência em seu começo, os passos são diversos e para diversos lados, mas com o tempo a comunidade dos cientistas vêm realizando pesquisas e buscando comprovar a efetividade de algoritmos de detecção de Fake News nos maiores portais sociais atuais, apesar das diversas nuances que existem na área, se com sucesso, eles podem diminuir a divulgação de notícias falsas em grandes quantidades.

4.1. CONSIDERAÇÕES DO CAPÍTULO

Neste capítulo foi abordado de forma mais transparente as grandes dificuldades da área do reconhecimento de padrões quando se trata de detecção de Fake News: O assunto ser muito recente, então faltam trabalhos e provas estatísticas, a definição do escopo ser muito discutida ainda, e a falta de dados numerosos para aplicação da Ciência de Dados. Foi discutido como a tendência está sendo pegar algoritmos e dados de iniciativas pré estabelecidas semelhantes, como os sistemas de detecção de Bots, e como parcerias com redes sociais pode ser um grande avanço para resolver vários dos problemas enfrentados atualmente.

5. CONCLUSÃO

Na busca de algumas instituições de abusarem da psicologia humana para divulgar informações falsas, recentemente na eleição presidencial estadunidense, que deixou o tema em voga, mas também vem de muitos anos antes, sendo a mídia uma massa de manipulação, surge o auxílio da Ciência de Dados de maneira a utilizar do reconhecimento de padrões para detectar Fake News e parar a sua divulgação.

Nesta monografia foi discutido o panorama histórico entre os dois temas, como a as notícias falsas sempre foram um problema para a humanidade e usadas como uma massa de manobra, e o surgimento de tecnologias que tornaram possível a ampla divulgação da informação, tornando mais difícil o trabalho de quem queria criar mentiras, mas tornando mais rápido o processo de sua divulgação. Ao mesmo tempo, mostramos o surgimento da Ciência de dados e como os aspectos que viriam a ser responsáveis pela área de

reconhecimento de padrões foram se desenvolvendo ao longo dos anos até abordarem o problema diretamente desde 2016.

Foi discutido uma definição mais formal do que é Fake News e como ela é debatida no meio acadêmico e pode gerar diversos problemas ao se desenvolver pesquisas e algoritmos no meio, e também a responsabilidade dos cientistas ao fazerem tais pesquisas por se tratar de um tema com diversas nuances que podem categorizar a detecção em censura.

Foram abordadas diferentes estratégias usadas hoje no meio para a detecção efetivas das Fake News, que estão divididas em três grandes campos: A análise do conteúdo, das fontes e a mudança nos incentivos que pessoas ou sites tem para compartilhar. Na primeira, onde analisa-se o conteúdo da notícia ou postagem em si, existem diferentes formas sendo feitas e testadas para fazer isso, entre elas as flags, os algoritmos óbvios e os baseados nas Wikipedia Hoaxes, que é um sistema de heurística estabelecido pela Wikipedia para determinar artigos falsos em sua database. Na detecção de fontes vimos que o maior foco no meio é a detecção de sistemas de bots, pois já existem uma boa base de testes e de pesquisas na área, e o desafio é usar desses sistemas para fazer um paralelo com a detecção especificamente de Fake News. Vimos então duas das maiores contribuições nesse meio, o BotOrNot e a Lei de Benford. Por fim, a modificação de incentivos que busca alterar a forma gratificante que Fake News são compartilhadas, tanto para sites que lucram ou querem fazer algum tipo de propaganda em cima dela, tanto para pessoas que acreditam naquela informação, e como alterar esse meio atual de forma a não ter esse incentivo.

Além de muitas estratégias dentre esses três pontos abordadas no capítulo 3, também vimos como um amplo maior as maiores dificuldades que a Ciência de Dados encontra nesse contexto, sendo a falta de dados numerosos e definições incertas de escopo do problema. Desafios esses que têm tendência de serem mais facilmente resolvidos com o tempo, por ser uma abordagem muito nova a ideia de detectar Fake News com reconhecimento de padrões. Foi mostrado como parcerias com redes sociais ou sistemas que já abordavam problemas semelhantes parece ser a tendência pela quantidade de dados disponíveis e pesquisas já feitas na área que podem ser usadas como um apoio.

REFERÊNCIAS BIBLIOGRÁFICAS

MCLACHLAN, Hugh. **Fake news is very far from being a novel phenomenon.** 2017. Disponível em: <http://www.heraldscotland.com/business_hq/opinion/15627541.Agenda__Fake_news_is_very_far_from_being_a_novel_phenomenon/>. Acesso em: 30 out. 2017.

PROVOST, Foster; FAWCETT, Tom. **Data Science for Business:** : What You Need to Know about Data Mining and Data-Analytic Thinking. New York: O'reilly, 2013. 384 p.

LINDEN, Sander van Der. Beating the Hell Out of Fake News. **Ethical Record**: Proceedings of the Conway Hall Ethical Society, Cambridge, v. 6, n. 122, p.4-7, dez. 2017.

WEISS, William. Press. In: WEISS, William. **History's Greatest Lies.** Massachusetts: Fair Winds Press, 2009. p. 28-41.

CLEVELAND, William S.. Data Science: an Action Plan for Expanding the Technical Areas of the Field of Statistics. **International Statistical Review**, [s.l.], v. 69, n. 1, p.21-26, abr. 2001. Wiley. http://dx.doi.org/10.1111/j.1751-5823.2001.tb00477.x.

PRESS, Gill. **A Very Short History Of Data Science.** 2013. Disponível em: <https://www.forbes.com/sites/gilpress/2013/05/28/a-very-short-history-of-data-science/#3038b63555cf>. Acesso em: 28 maio 2013.

BISHOP, Christopher M .. **Pattern Recognition and Machine Learning.** New York: Springer, 2006. 738 p. "Pattern recognition has its origins in engineering, whereas machine learning grew out of computer science. However, these activities can be viewed as two facets of the same field, and together they have undergone substantial development over the past ten years.".

VAPNICK, V.n; CHERVONENKIS, A. Ya.. Theory of Pattern Recognition. **Statistical Problems Of Learning.** Nauka, p. 0-0. maio 1974.

KUDO, Mineichi; SKLANSKY, Jack. Comparison of algorithms that select features for pattern classifiers. **Pattern Recognition**, [s.l.], v. 33, n. 1, p.25-41, jan. 2000. Elsevier BV. http://dx.doi.org/10.1016/s0031-3203(99)00041-2.

PATTON, Lydia. **Philosophy, Science, and History:** A Guide and Reader. Virginia: Routledge, 2014. 482 p.

BROECK, Jan van Den et al. Data Cleaning: Detecting, Diagnosing, and Editing Data Abnormalities. **Plos Medicine**, [s.l.], v. 2, n. 10, p.200-267, 6 set. 2005. Public Library of Science (PLoS). http://dx.doi.org/10.1371/journal.pmed.0020267.

KUMAR, Srijan; WEST, Robert; LESKOVEC, Jure. Disinformation on the Web. **Proceedings Of The 25th International Conference On World Wide Web - Www '16**, [s.l.], v. 0, n. 0, p.591-602, out. 2016. ACM Press. http://dx.doi.org/10.1145/2872427.2883085.

OSBORNE, Jason W.. **Best Practices in Data Cleaning:** A Complete Guide to Everything You Need to Do Before and After Collecting Your Data. Thousand Oaks: Sage Publications, 2012.

TSCHIATSCHEK, Sebastian et al. Fake News Detection in Social Networks via Crowd Signals. **Companion Of The The Web Conference 2018 On The Web Conference 2018 - Www '18**, [s.l.], v. 0, n. 0, p.0-8, abr. 2018. ACM Press. http://dx.doi.org/10.1145/3184558.3188722.

FREEMAN, David Mandell. Can You Spot the Fakes? **Proceedings Of The 26th**

International Conference On World Wide Web - Www '17, [s.l.], v. 0, n. 0, p.1093-1102, maio 2017. ACM Press. http://dx.doi.org/10.1145/3038912.3052706.

VAROL, Onur. Online Human-Bot Interactions: Detection, Estimation, and Characterization. **Icwsm'17**, Cornell, v. 0, n. 0, p.0-10, maio 2017.

DUNHAM, Ken; MELNICK, Jim. **Malicious Bots:** An Inside Look into the Cyber-Criminal Underground of the Internet. Auerbach: Crc Press, 2008. 168 p.

FEWSTER, R. M.. A Simple Explanation of Benford's Law. **The American Statistician**, [s.l.], v. 63, n. 1, p.26-32, fev. 2009. Informa UK Limited. http://dx.doi.org/10.1198/tast.2009.0005.

GOLBECK, Jennifer. Benford’s Law Applies to Online Social Networks. **Plos One**, [s.l.], v. 10, n. 8, p.8-10, 26 ago. 2015. Public Library of Science (PLoS). http://dx.doi.org/10.1371/journal.pone.0135169.

GOLBECK, Jennifer. Incomplete Article. DC Data Science Conference, 2018.