

# O Paradoxo da Viralização de Informação Criptografada no *WhatsApp*

Carolina Coimbra Vieira<sup>1</sup>, Philipe de Freitas Melo<sup>1</sup>,  
Pedro O. S. Vaz de Melo<sup>1</sup>, Fabrício Benevenuto<sup>1</sup>

<sup>1</sup>Departamento de Ciência da Computação  
Universidade Federal de Minas Gerais (UFMG)  
Belo Horizonte – MG – Brasil

{carolcoimbra, philipe, olmo, fabricio}@dcc.ufmg.br

**Abstract.** *WhatsApp is a mobile communication system that allows people to interact through groups. In this work, we analyze the dissemination of information within a group network that simulates the WhatsApp network. The built network considers two types of groups: organic groups, formed by friends and family, and artificial groups that are usually created with the purpose of being a mean of spreading certain subject or event, such as political campaigns. We analyzed the speed with which information is spread in this network considering the epidemiological model Susceptible-Infected (SI). We then deepen our analysis in order to identify parameters that cause this scattering to be partially controlled in order to make it difficult to propagate fake news in these networks. Our results quantify the viralization ability of content in WhatsApp and identify aspects that could limit such ability to prevent the platform from being abused in election periods.*

**Resumo.** *O WhatsApp é um sistema de comunicação móvel que permite que pessoas interajam através de grupos. Neste trabalho, analisamos a disseminação de informações dentro de uma rede de grupos que simula a rede do WhatsApp. A rede construída considera dois tipos de grupos: grupos orgânicos, formados por amigos e familiares, e grupos artificiais que, em geral, são criados com o objetivo de ser um meio de divulgação de determinado assunto ou evento, como por exemplo, campanhas políticas. Analisamos a velocidade com que se dá o espalhamento de informação nessa rede considerando o modelo epidemiológico Suscetível-Infectado (SI). Em seguida aprofundamos nossa análise buscando identificar parâmetros que fazem com que esse espalhamento seja parcialmente controlado de forma a dificultar a propagação de notícias falsas nessas redes. Nossos resultados quantificam a capacidade de viralização de um conteúdo no WhatsApp e identificam aspectos que poderiam limitar tal capacidade para evitar que a plataforma seja abusada em períodos eleitorais.*

## 1. Introdução

O *WhatsApp* é um sistema de comunicação móvel que, desde a sua criação em 2009, vem mudando a forma como os usuários de *smartphones* se comunicam. Atualmente, o *WhatsApp* é o aplicativo de troca de mensagens mais popular em termos de números de

usuários<sup>1</sup>, ultrapassando a marca de 1,5 bilhão de usuários ativos<sup>2</sup>. E, além de ser muito utilizado para manter contato com amigos e familiares, negócios, ler notícias e se informar, o *WhatsApp* se tornou uma importante plataforma de disseminação de informação e mobilização social. Isso porque, dentre as principais funcionalidades do *WhatsApp* estão a possibilidade de enviar e encaminhar mensagens para múltiplos usuários e criar grupos.

Por essas peculiaridades, o *WhatsApp* gera uma controvérsia relacionada a suas características de anonimidade e viralização. Esse conflito se deve ao fato de podermos encarar o *WhatsApp* de duas maneiras diferentes, como uma empresa de tecnologia, ou como uma plataforma midiática. Como plataforma de tecnologia, ele garante a anonimidade do usuário e uma segurança através da criptografia de seus dados. Como plataforma midiática, assim como um canal de rádio ou televisão, ela transmite a informação e divulga conteúdo por meio de suas funções de *broadcast*<sup>3</sup> e *forward*<sup>4</sup> que permitem uma viralização das mensagens. Portanto, mensagens enviadas de forma anônima alcançam milhares de pessoas rapidamente e sem nenhuma regulamentação ética ou legal deste conteúdo disseminado, promovendo, por exemplo, o espalhamento de notícias falsas. Essas críticas já levaram o aplicativo a implementar restrições na forma de encaminhamento de mensagens<sup>5</sup> como meio de controlar a velocidade de espalhamento do conteúdo. Porém, não há estudos que mostram qual o impacto dessas limitações, nem se os números escolhidos são suficientes para lidar com conteúdo viral.

Além disso, o aplicativo permite criação de grupos, conectando diversas pessoas simultaneamente, deixando o traço de conversa interpessoal, tal como o SMS, e virando um meio de comunicação em massa, assim como o *Facebook* ou outras redes sociais. Os grupos criados no *WhatsApp* possuem um limite de 256 usuários e podem ser privados ou públicos. No caso dos grupos privados, novos membros devem ser adicionados por um membro que assume o papel de administrador do grupo. Já para os grupos públicos, o acesso se dá por meio de *links* de convite. E, em geral, esses grupos surgem com o propósito de discutir assuntos específicos como política.

Nesse contexto, o *WhatsApp* tem sido apontado como uma das principais ferramentas de disseminação de informações e notícias pela sociedade. Através do encaminhamento de mensagens ou criação de grupos, o *WhatsApp* foi protagonista em alguns eventos pelo Brasil, como na greve dos caminhoneiros<sup>6</sup> [Resende et al. 2018] e nas eleições presidenciais em 2018 [Resende et al. 2019], e no mundo, como o espalhamento de notícias falsas com boatos sobre sequestros de crianças na Índia [Chakrabarti et al. 2018] e no México<sup>7</sup>.

Neste trabalho, abordamos o desafio de compreender os efeitos das características específicas de grupos e compartilhamento do *WhatsApp* na difusão e espalhamento de informação dentro de sua rede. Mais especificamente procuramos responder as seguintes questões de pesquisa: **(RQ1)**: Qual o impacto dos grupos na propagação de informação

---

<sup>1</sup><https://www.statista.com/>

<sup>2</sup><https://blog.whatsapp.com/10000631/Conectando-um-bilho-de-usuarios-todos-os-dias?>

<sup>3</sup>Uma lista de contatos pode ser criada para enviar mensagens para até 256 contatos de uma só vez. E, podem ser criadas, no máximo, 5 listas distintas.

<sup>4</sup>Uma mensagem pode ser encaminhada para até 5 pessoas na Índia e 20 pessoas no resto do mundo.

<sup>5</sup><https://blog.whatsapp.com/10000647/Mudan%C3%A7as-no-encaminhamento-de-mensagens>

<sup>6</sup><https://www.bbc.com/portuguese/brasil-44325458>

<sup>7</sup><https://www.bbc.com/portuguese/salasocial-46206104>

na estrutura de rede do *WhatsApp*? **(RQ2)**: É possível controlar o espalhamento de informação com as limitações de *forward* ou *broadcast* impostas pelo aplicativo?

Para responder a cada uma delas, fizemos uma caracterização inicial a partir de dados coletados de grupos públicos. Então, propomos um modelo de geração de uma rede que consiga representar melhor as características e grupos presentes no *WhatsApp*. Também realizamos diversos experimentos a fim de mensurar a viralização, utilizando o modelo epidemiológico Suscetível-Infetado (SI). Finalmente, tentamos identificar condições onde é possível controlar a propagação na rede variando alguns parâmetros que refletem na forma com que ocorre o espalhamento.

O restante do artigo está organizado da seguinte forma: na seção 2 descrevemos os trabalhos relacionados. Então, na seção 3 abordamos a metodologia utilizada para modelar a rede do *WhatsApp* e respondermos as questões de pesquisa levantadas. Os experimentos que mostram o impacto dos parâmetros de *forward* e *broadcast* na velocidade de propagação de informação na rede são mostrados na seção 4. Por último, na seção 5, discutimos nossas observações e conclusões finais sobre o trabalho.

## 2. Trabalhos Relacionados

Nos últimos anos, muitos estudos investigam como redes sociais são exploradas na organização de movimentos políticos, como o papel das redes sociais durante a Primavera Árabe no Oriente Médio [Howard and Hussain 2011] e as diferentes narrativas construídas no Twitter sobre os Capacetes Brancos na Síria [Starbird et al. 2018]. Além disso, há uma série de esforços recentes que investigam o papel de campanhas políticas através das redes sociais, principalmente focados nas eleições presidenciais dos EUA de 2016. Como exemplo, há uma série de esforços que investigam a criação de *bots* no *Twitter* e o seu papel no engajamento de usuários no discurso político [Freitas et al. 2015, Bessi and Ferrara 2016]. Outros trabalhos [Ribeiro et al. 2019, Andreou et al. 2019, Speicher et al. 2018] avaliaram o uso da plataforma de propagandas do *Facebook* para a realização de campanhas políticas que exploram o marketing direcionado como forma de disseminar propagandas falsas ou sobre temas divisíveis, incitando polarização e ódio [Mondal et al. 2017] nas redes sociais. Outros esforços visam explorar estratégias para detecção automática de notícias falsas [Reis et al. 2019]. Nosso trabalho é complementar aos esforços acima, pois investigamos a capacidade de viralização de um aplicativo que foi bastante explorado na disseminação de notícias falsas no Brasil.

O *WhatsApp* é usado por mais da metade da população brasileira, com cerca de 120 milhões de usuários no Brasil<sup>8</sup>. Na Índia, mais de 94% de todos os dispositivos *Android* possuem o aplicativo instalado [Garimella and Tyson 2018] e é a plataforma de mídia social mais popular junto com o *Facebook* no Oriente Médio [Radcliffe and Lam 2018]. Estudos recentes já demonstram o impacto dessa mídia social em diversos cenários. [Resende et al. 2019] analisaram a disseminação de informação através do envio de mídias como imagens, áudios e vídeos no *WhatsApp* utilizando um extenso conjunto de dados proveniente de grupos políticos públicos durante a greve dos caminhoneiros e nas eleições presidenciais do Brasil em 2018, encontrando uma grande presença de desinformação criada e compartilhada no aplicativo e analisando seu espa-

---

<sup>8</sup><https://link.estadao.com.br/noticias/empresas,whatsapp- chega-a-120-milhoes-de-usuarios-no-brasil,70001817647>

lhamento nessa rede. [Moreno et al. 2017] apontam o benefício do uso do *WhatsApp* como fonte de informação para monitorar eleições em Gana [Moreno et al. 2017]. Já [Malka et al. 2015] focaram em como cidadãos de Israel usam *WhatsApp* durante período de guerra, no qual observaram que a plataforma desempenha um papel central na vida de seus usuários em cenários de conflito, funcionando como um canal multifuncional de comunicação tanto em massa como também interpessoal.

Outra dentre as principais características que diferem o *WhatsApp* das mensagens de texto SMS está na ferramenta de criação de grupos. Desta forma, alguns estudos estão voltados em como se dá essa comunicação baseada em grupos dentro do *WhatsApp* [Seufert et al. 2015, Seufert et al. 2016]. [Rosenfeld et al. 2018] realizaram uma análise do comportamento de 100 usuários para inferência de informações demográficas como idade e gênero. Alguns passos em direção a uma melhor compreensão desta rede também foram dados em [Garimella and Tyson 2018], no qual os autores caracterizaram dados de grupos públicos, apresentando uma metodologia de coleta do aplicativo. [Melo et al. 2019] desenvolveram um sistema onde coletaram e exploraram o envio de imagens, mensagens, URL's, áudios e vídeos em mais de 300 grupos públicos no Brasil e mais de 800 grupos da Índia, evidenciando os conteúdos mais compartilhados que foram utilizados por diversos jornalistas para monitorar eleições no Brasil. Porém, nenhum trabalho avalia o impacto das características de viralização de mensagens na disseminação de informação na rede do *WhatsApp*.

Pelo lado do espalhamento viral, outros trabalhos usam os modelos epidemiológicos para prever tendências de *retweetar tweets* [Feng et al. 2015] ou para explicar padrões de propagação da informação no *Flickr* [Cha et al. 2012]. Outro modelo de predição desenvolvido a partir de modelos epidemiológicos, proposto em [Guha et al. 2004], mostra que um pequeno número de confiança/desconfiança expresso por indivíduos em uma rede permite prever a confiança entre duas pessoas. E, por fim, no trabalho de [Khurana and Kumar 2018], os modelos epidemiológicos são aplicados no contexto de disseminação de notícias falsas no *Whatsapp*. Porém, os parâmetros do modelo são estimados e somente um cenário é considerado. Nosso trabalho por outro lado, além de considerar os dois tipos de grupos que existem no *WhatsApp*, modela uma série de cenários possíveis a partir da variação dos principais parâmetros que fazem com que a rede do *WhatsApp* seja viral.

### 3. Metodologia

Nesta seção, apresentamos a metodologia seguida para modelar a rede do *WhatsApp* baseado na topologia de redes sociais somada às descobertas a partir dos dados coletados de grupos públicos políticos durante as eleições. Primeiro, descrevemos e analisamos os dados utilizados provenientes do *WhatsApp* que são usados como parâmetro para reconstrução da rede. Depois, discutimos sobre a estrutura da rede do *WhatsApp* e suas semelhanças e diferenças com outras redes sociais. Exploramos, então, a construção de um modelo generativo para criar um grafo condizente com a rede de usuários pertencentes ao *WhatsApp* e que consiga representar bem características peculiares da rede como a presença de grupos de conversa. Também propomos aqui uma divisão da rede em dois diferentes tipos de grupos: os Orgânicos e os Artificiais.

Além disso, abordaremos os passos seguidos para a simulação do efeito de

viralização de mensagens tentando emular as limitações de *forward* e *broadcast* que ocorrem dentro desta rede. Para isso, utilizamos o modelo suscetível-infectado (SI) para realização de experimentos que medem a velocidade e alcance desse espalhamento de informação dentro das redes propostas.

### 3.1. Caracterização do *WhatsApp*

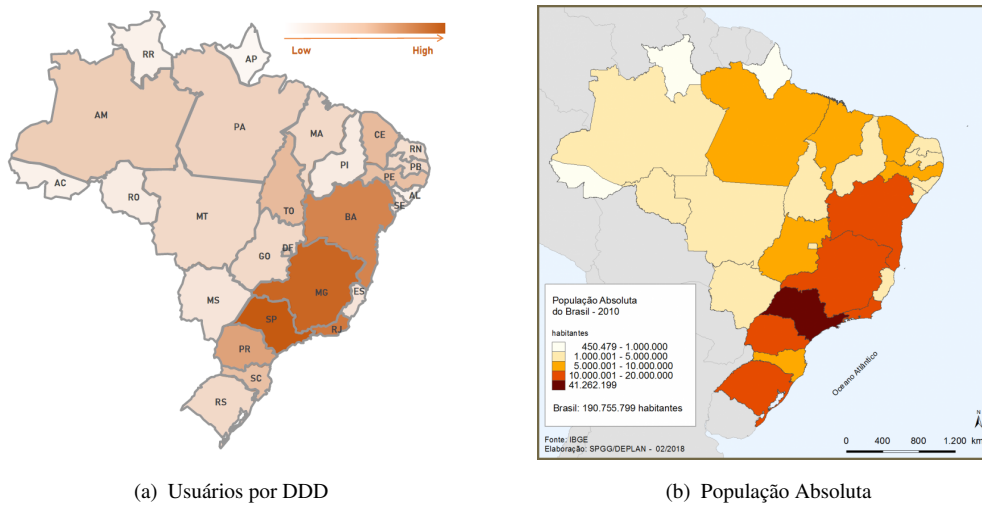
Para entender melhor a estrutura da rede do *WhatsApp* e sua ferramenta de criação de grupos, realizamos uma caracterização de suas propriedades básicas buscando identificar comportamentos e vieses dos dados que diferenciam a rede de grupos do *WhatsApp* das demais redes sociais como *Facebook* e *Twitter*. Foram utilizados os dados de [Resende et al. 2019] coletados durante o período eleitoral entre 16 de Setembro e 05 de Outubro de 2018 utilizando a ferramenta *WebWhatsAppAPI*<sup>9</sup>, que coleta as mensagens utilizando a versão web do *WhatsApp*. Esses dados se referem somente às imagens compartilhadas durante o período das eleições presidenciais em 364 grupos políticos públicos monitorados pelo trabalho.

A primeira análise consiste em identificar os padrões geográficos contidos nos dados. Como cada usuário está associado a um número de telefone, é possível localizar geograficamente os usuários através de seu código DDD. A Figura 1 apresenta o mapa coroplético das localizações dos 10 mil usuários coletados distribuídos pelas unidades federativas do Brasil. Cores mais escuras indicam maior concentração de usuários naquele estado. Os estados com maior número de usuários incluem SP (1322), MG (1116), RJ (992) e BA (905). Esses valores confirmam o viés geográfico da distribuição real 1(b) da população sobre o território brasileiro, o que demonstra que os dados possuem uma amostra de usuários semelhante à distribuição populacional brasileira. Entretanto, podemos observar maiores discrepâncias para os estados do RS (275), que aparece sub-representado, TO (479) e DF (380), que possuem proporcionalmente mais usuários do que a distribuição de população. Como tratam-se de dados políticos, relacionamos esse aumento no DF à sua proximidade da vida política do país. Já Tocantins aparece com uma concentração também acima do normal devido a uma grande quantidade de grupos monitorados referentes àquele estado.

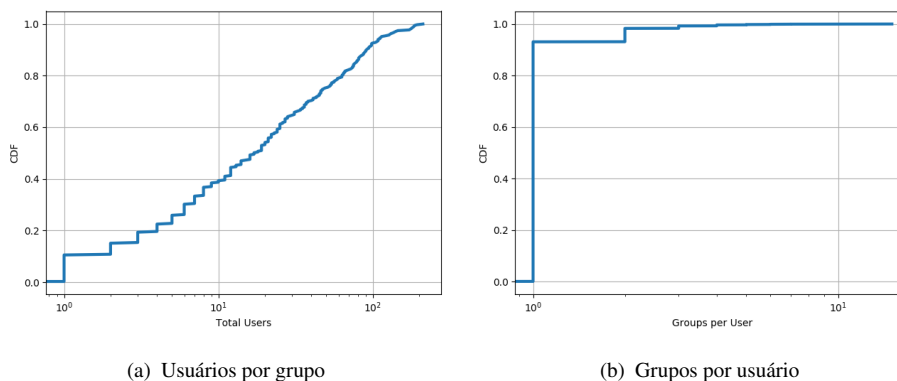
Além desta caracterização inicial, mostrando uma boa amostragem da população, também analisamos as distribuições de usuários por grupos para entendermos melhor o comportamento da rede do *WhatsApp*. A Figura 2 mostra as duas curvas de distribuições (CDF), sendo 2(a) a quantidade de usuários ativos em cada grupo e 2(b) a quantidade de grupos públicos que cada usuário participa. A primeira mostra a população dos grupos em termos de usuários ativos, ou seja, usuários que postaram pelo menos uma mensagem no grupo durante o período eleitoral. Podemos observar que 50% dos grupos possuem até 20 usuários, mas há grupos, cerca de 10%, que ultrapassam os 100 usuários, chegando, no máximo, em um grupo com 211 membros. Esses valores são reflexos das limitações que a ferramenta do *WhatsApp* impõe de até 256 membros num grupo padrão, pois este valor se aproxima do limite encontrado nos dados. Além disso, é uma evidência também do comportamento dos usuários de grupos públicos, acima do reportado pelo próprio *WhatsApp*. Enquanto encontramos uma média de 34 usuários por grupos, a maioria dos grupos de forma geral no Brasil tem cerca de apenas 6 pessoas<sup>10</sup>.

<sup>9</sup><http://github.com/mukulhase/WebWhatsapp-Wrapper>

<sup>10</sup><https://newsroom.fb.com/news/h/how-whatsapp-is-fighting-misinformation-in-brazil/>



**Figura 1. Comparação populacional entre a geolocalização dos usuários do *WhatsApp* baseado no código DDD de telefone e população do Brasil.**



**Figura 2. *Cumulative Distribution Function (CDF)* para distribuição de usuários e grupos.**

A segunda curva, paralelamente, mostra a distribuição da quantidade de grupos que um usuário participa. Aqui, temos um comportamento bem evidente em que mais de 90% dos usuários foram encontrados em apenas um único grupo dentre os monitorados. Porém, temos também alguns poucos usuários participando cada um de mais de 10 grupos. Mesmo que a maioria dos usuários esteja conectada a poucos grupos, alguns usuários membros de vários grupos se tornam “hubs” e conseguem fazer o papel de ponte, espalhando a informação para os demais usuários, nos dando as primeiras pistas do processo de viralização no *WhatsApp*, semelhante ao que ocorre nas demais redes sociais.

### 3.2. Estrutura de Rede do *WhatsApp*

A partir dos resultados da caracterização, podemos perceber que o *WhatsApp* é uma mídia social poderosa, capaz de levar uma mesma mensagem a vários usuários espalhados pelo país num período muito curto de tempo, de forma semelhante a outras redes como o *Twitter* e o próprio *Facebook*. Isso acontece devido sua topologia de rede com a formação de grupos de conversa, sendo vários destes com uma grande quantidade de membros. Ainda, é possível observar alguns usuários participando de vários grupos ao mesmo tempo, podendo compartilhar mensagens e ultrapassar facilmente as fronteiras dos grupos e transi-

tando rapidamente através da rede. Essas características possibilitam à população o uso do *WhatsApp* como fonte de notícias e informação.

Porém, outros dados mostram também que mais de 90% das mensagens enviadas no *WhatsApp* no Brasil são conversas individuais e a maioria dos grupos é composto de apenas 6 pessoas<sup>11</sup>. Estes números evidenciam um grande volume de conversas ainda no nível interpessoal numa esfera mais particular, o que difere bastante dos dados referentes aos grupos públicos coletados durante as eleições. Nestes grupos públicos, diferente do que acontece no restante do *WhatsApp*, há uma quantidade muito maior de pessoas e um fluxo bem intenso de informação tanto dentro do grupo, como também para fora dele, interagindo com outros grupos. Assim sugerimos duas categorias baseadas na formação e comportamento de grupos do aplicativo: os grupos Orgânicos e os Artificiais.

Consideramos grupos orgânicos aqueles criados devido a uma proximidade inerente da própria rede social de amigos dos usuários. Grupos como grupos familiares, grupos de turmas de alunos, de trabalho, associações e clubes, em que os usuários possuem uma proximidade mais natural e que, geralmente, possuem alguma relação fora do aplicativo. Por outro lado, os grupos artificiais são grupos maiores, em geral, públicos e que atraem membros diversificados que se unem por algum interesse em comum, como religião, futebol e política. Os usuários conectados à esses grupos não necessariamente possuem alguma relação de amizade externa ao grupo.

Com essa divisão, procuramos distinguir e analisar os dois usos distintos do *WhatsApp*: o uso interpessoal, feito na conversa par-a-par e pelos grupos orgânicos onde usuários se mantêm conectados com familiares e amigos, numa relação muito mais particular que requer segurança e anonimato na rede; e os grupos artificiais, onde existe uma comunicação em massa em que o objetivo do usuário é ler notícias, se manter bem informado dos acontecimentos da sociedade, realizar um ativismo virtual ou promover algum discurso ou ideia. Acreditamos que com essa separação deixamos mais transparente nossa metodologia e mais próximo do que acontece no cenário real. A seguir, apresentaremos a construção de um modelo para recriar uma rede similar à rede de grupos do *WhatsApp*, considerando esta divisão entre grupos orgânicos e artificiais, a partir de uma rede social.

### 3.2.1. Gerador de Grupos Orgânicos

Os grupos orgânicos foram definidos como os formados devido a uma proximidade real entre seus membros, no qual eles compartilham um grau de relacionamento que vai além daquele dentro do aplicativo. Portanto, eles são criados a partir da rede de amigos de um usuário durante seu convívio diário. O primeiro passo para simular esta estrutura de rede, então, é conseguir simular também a rede social daqueles usuários e depois inferir os grupos originados a partir dela. Para esta tarefa, existem diversos algoritmos que geram grafos tentando simular o comportamento de redes sociais, com objetivos e regras específicas que geram estruturas bem variadas. Neste trabalho, utilizamos alguns destes métodos para tentar identificar aquele que seria o mais adequado para a criação da rede de grupos, além de também incluir um grafo de rede social real, o do Flickr<sup>12</sup>, como base

<sup>11</sup>Declaração do vice-presidente do *WhatsApp*, disponível em <https://newsroom.fb.com/news/h/how-whatsapp-is-fighting-misinformation-in-brazil/>

<sup>12</sup>O *Flickr* é um serviço de hospedagem de imagem e serviço de hospedagem de vídeo criado em 2004 pela Ludicorp.

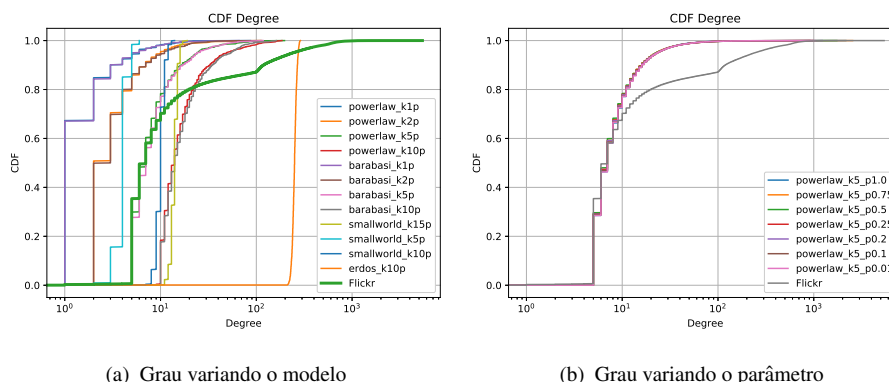


Figura 3. Distribuição de graus dos nós da rede gerada pelos diferentes métodos e variando alguns parâmetros.

de comparação.

Em nossos experimentos, foram comparados alguns métodos de geração de grafos de redes heterogêneas (*scale-free*) [Barabási et al. 2016] da biblioteca *networkX*<sup>13</sup> disponível em Python. Dentre esses métodos foram comparados o *preferential attachment* de Barabasi-Albert, o algoritmo de Holme e Kim para grafos escaláveis com distribuição *power law* de graus e agrupamento médio aproximado, o modelo *Small World* e o modelo binomial de Erdős-Rényi .

Os resultados obtidos em cada modelo foram comparados com a rede do *Flickr* disponibilizada por [McAuley and Leskovec 2012]. A rede do *Flickr* foi escolhida por se tratar de uma rede menor e menos densa do que grafos complexos como o do *Facebook* ou do *Twitter* e permitir então comparar o grafo gerado artificialmente com um cenário real como número mais reduzido de nós. A Figura 3 mostra a distribuição de graus dos nós do *Flickr* e de cada modelo utilizado . Como podemos ver, nenhum modelo consegue reproduzir perfeitamente os dados reais, porém, os modelos de Barabasi-Albert e *Power Law* possuem o comportamento mais próximo de um cenário real, quando o parâmetro  $k = 5$ . Além disso, apesar da rede do *Flickr* possuir uma quantidade maior de nós com grau alto, quando novas arestas forem adicionadas à rede *powerLaw\_k5* devido à criação dos grupos, o aumento no grau dos nós fará com que ela se aproxime um pouco mais da rede real. Além disso, mesmo as redes geradas possuindo uma menor densidade, com menos graus de alto grau que o *Flickr*, esses modelos foram preferíveis, uma vez que mais arestas ainda serão adicionadas ao modelo para gerar o comportamento de grupos, aumentando posteriormente a densidade dessa rede.

Em sequência, com esta rede de amizade montada, é necessário identificar os grupos orgânicos presentes nela, adicionando assim novas arestas. Como definimos esses grupos como aqueles criados por uma distância naturalmente curta entre os seus participantes, podemos utilizar esta rede como base para detectarmos comunidades e criar grupos a partir delas. Para este passo, alguns métodos de detecção de comunidades foram testados a fim de ver a melhor forma de criar os grupos [Barabási et al. 2016]: o algoritmo de *k*-clique, o de maximização modular de Clauset-Newman-Moore, o de propagação de rótulos, o *Fluid Communities* e o método de Girvan–Newman

<sup>13</sup><https://networkx.github.io/documentation/stable/>



Considerando o tempo de processamento do método, a quantidade e tamanho das comunidades encontradas, e a rede *powerLaw\_k5* como entrada, o método de Clauset-Newman-Moore foi escolhido para modelar o processo de criação de grupos orgânicos do *WhatsApp*. Cada comunidade identificada pelo método é então considerada um grupo orgânico (tal como grupos de trabalho, de estudo, ou família). Finalmente, adicionamos as arestas faltantes a esse grupo a fim de transforma-lo numa clique, conectando todos os membros entre si, tal qual aconteceria no ambiente do *WhatsApp*.

### 3.2.2. Gerador de Grupos Artificiais

Os grupos artificiais são, por outro lado, criados com um *link* público e acessível para qualquer usuário entrar. Eles podem ser para divulgação de determinado assunto ou evento, ou mesmo compartilhar interesses mais amplos na sociedade, mas tem objetivos de alcançar um maior número de pessoas possível. Portanto, os membros desses grupos não necessariamente se conhecem ou possuem alguma proximidade fora do aplicativo. Para considerar essa topologia de grupo em nossa rede gerada, foram utilizados as análises das distribuições apresentadas nas Figuras 2(a) e 2(b) dos dados de [Resende et al. 2019] de mais de 350 grupos públicos de *WhatsApp* para estimar quantidade de grupos e membros a serem utilizados.

Esses dados de quantidade de grupos por usuários e a quantidade de usuários por grupos foram utilizados para estimar uma probabilidade de cada um dos nós da rede se tornar membro de um grupo público, respeitando o limite de 256 membros por grupo do *WhatsApp*. Dessa forma, criamos um conjunto de grupos artificiais com uma distribuição de membros aproximada dos dados reais. Por fim, assim como ocorre nos orgânicos, conectamos todos usuários de um grupo entre si, formando uma clique igual temos no cenário real.

### 3.3. Modelo Suscetível-Infetado

Com a rede pronta, precisamos de um modelo capaz de medir o poder de viralização entre os usuários. Utilizamos, então, o modelo Suscetível-Infetado (SI). Este é um dos modelos epidemiológicos mais simples, já muito utilizado para avaliar a disseminação de informação em redes sociais [Keeling and Eames 2005]. No modelo SI existem duas fases no processo de disseminação da epidemia: Suscetível (S) e Infetado (I).  $S$  corresponde à proporção da população que é suscetível ou, nesse caso, que ainda não foi exposta a determinado conteúdo. E,  $I$  corresponde à proporção da população que está infetada, ou seja, já foi exposta ao conteúdo. Inicialmente, algumas suposições são necessárias, como a proporção de pessoas infetadas,  $x_0$ , a proporção de pessoas que são suscetíveis,  $S_0$  e a taxa de transmissão  $\beta$ , que incorpora a taxa de encontro entre indivíduos suscetíveis e infetados juntamente com a probabilidade de transmissão. Considerando ainda uma “população fechada”, sem nascimentos, mortes ou migrações, onde a proporção de nós infetados sempre suscetíveis soma 1 e  $\beta SI$  é usado como termo de transmissão.

A fração de infetados segue um crescimento logístico caracterizado por sua curva em formato de “S”.  $x_0$  é o valor inicial de I. A curva cresce exponencialmente logo após o primeiro indivíduo infetado e, em seguida, satura quando não existem mais indivíduos suscetíveis que podem ser alcançados. De forma complementar, a curva representando a

quantidade de indivíduos suscetíveis decai conforme o aumento no número de indivíduos infectados. Nesse modelo, o conjunto de usuários infectados (I) propaga informação para seus vizinhos que, por sua vez, possuem uma probabilidade de acreditar e repassar aquela informação. Utilizamos esse modelo para avaliar a velocidade de espalhamento de uma informação no *WhatsApp*, considerando os usuários como o grupo suscetível e iniciando alguns deles como infectados como sementes de criação de um conteúdo na rede. Com o parâmetro  $\beta$  manipulamos a taxa de infecção de modo a emular as limitações de *forward* e *broadcast* que existe dentro da rede como mostrado nos resultados. Para isso, estabelecemos uma métrica de penalização baseada na proporção de vértices do grafo com grau maior que o limite de envio estabelecido (5 e 20 para *forward* e 256 para *boradcast*), quanto maior a proporção, mais penalizada será a transmissão no modelo.

#### 4. Resultados

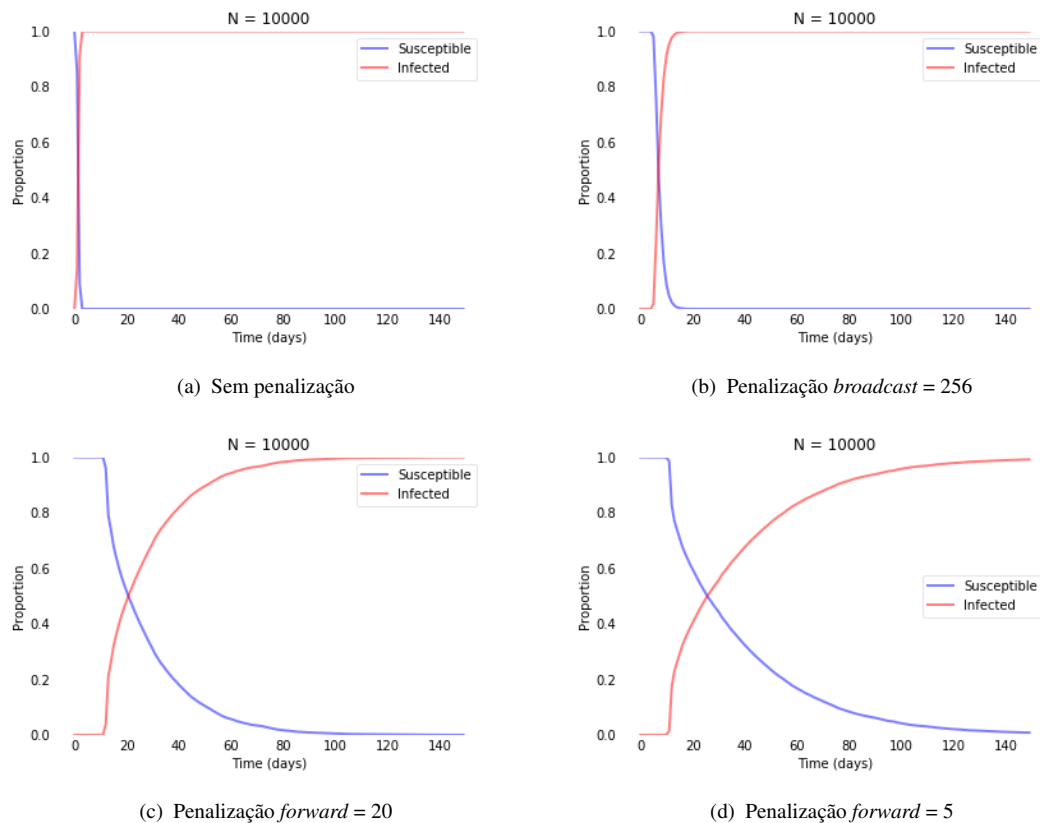
Para explorar a relação entre a topologia das redes de grupos e a velocidade de disseminação de informação na rede, foram realizados testes aplicando o modelo epidemiológico descrito na seção 3.3 às redes construídas seguindo o modelo de geração de redes de grupos proposto na seção 3.2. Além das redes geradas a partir da adição de grupos orgânicos e artificiais ao grafo *Power Law*, a rede social real do *Flickr* também foi comparada. A figura 4 mostra as curvas do modelo SI para algumas simulações realizadas variando as penalizações para *broadcast* e *forward*. É possível perceber que o tempo necessário para a disseminação completa de uma informação na rede aumenta na medida em que as penalizações se tornam maiores.

Com exceção da rede do *Flickr*, todas as redes de grupos testadas foram geradas a partir do grafo  $G$  que representa uma rede *Power Law* com dez mil nós, grau médio igual a 5 e probabilidade de clusterização igual a 0.25. Além disso, para o modelo SI, foi fixado uma taxa de espalhamento ( $\beta = 0.7$ ) conforme estimado por [Khurana and Kumar 2018].

A Figura 5 mostra os resultados em termos do tempo (quantidade de passos de simulação) necessário para infectar completamente cada uma das configurações de rede avaliadas. Os gráficos mostram a média e o desvio-padrão dos resultados para 10 execuções do modelo SI.

Podemos observar na Figura 5(a) que, na rede do *Flickr*, o tempo para a infecção completa da rede é bem maior do que nas de grupos geradas pelo modelo proposto. Considerando somente a rede *Power Law* com a adição de grupos orgânicos ( $G_{org}$ ), o tempo cai pela metade. O mesmo acontece quando se adiciona apenas os grupos artificiais à rede *Power Law* ( $G_{art}$ ). Já na rede que possui tanto grupos orgânicos quanto artificiais ( $G_{org\_art}$ ), o tempo de espalhamento é bem similar àquele da rede  $G_{org}$ .

O *WhatsApp* possui uma limitação no tamanho dos grupos, portanto, também foram realizadas simulações variando a quantidade de usuários por grupo considerando um cenário com 50 grupos artificiais.  $G_{org\_art}$  representa a rede de grupos seguindo a distribuição dos dados de [Resende et al. 2019],  $G_{org\_art\_g6}$  limita o tamanho dos grupos em 6 participantes, valor próximo à média geral apontada pela empresa e  $G_{org\_art\_g256}$  representa o cenário onde todos os grupos criados possuem o total de 256 participantes. É possível perceber que, o tamanho dos grupos influencia na velocidade com que a informação é disseminada na rede. Considerando os grupos de tamanho 256, por exemplo, percebe-se que o tempo de disseminação é reduzido em quase metade



**Figura 4. Simulações do modelo SI para a disseminação de informação na rede do *WhatsApp* com penalizações para *broadcast* e *forward*.**

do tempo das demais. Ou seja, quando a rede possui grupos maiores, a infecção acontece muito mais rapidamente.

Além do tamanho dos grupos, testamos também as limitações de compartilhamento da ferramenta do *WhatsApp* para quantidade de contatos na lista de *broadcast* e *forward*. Para isso, traduzimos essas limitações como penalizações no parâmetro  $\beta$ , baseado na quantidade média de nós que possuem um grau maior que o máximo estabelecido para cada tipo de redirecionamento de mensagem. Na Figura 5(b), além de considerar o modelo SI com  $\beta$  fixo igual a 0.7, foram variadas as penalizações de acordo com os limites estabelecidos pelo *WhatsApp* como sendo igual a 256 contatos por lista de *broadcast* e com limites de *forward* de no máximo 20 e 5 como aplicado na Índia. Com essas penalizações, vemos que o limite de *broadcast* possui um impacto muito pequeno no tempo de disseminação de informação na rede. Porém, para os limites de *forward* existe um barramento muito maior na infecção quando temos os grupos orgânicos, mas quase irrelevante com apenas os grupos artificiais. Isso acontece porque nas configurações dos grupos orgânicos, existem muito mais usuários que são limitados pelo número de vizinhos, portanto, a penalização na taxa de infecção acaba sendo maior, pois mais usuários terão de escolher dentre seus “amigos” quais ele poderá passar a informação, enquanto sem os orgânicos, a maioria dos usuários ainda poderá agir livremente.

Finalmente, quando comparamos a limitação de *forward* de 20 e de 5, vemos pouca diferença no tempo de infecção total das redes, com leve aumento, porém ainda assim sem muito efeito nos grupos artificiais apenas. Somente com os dois tipos de gru-

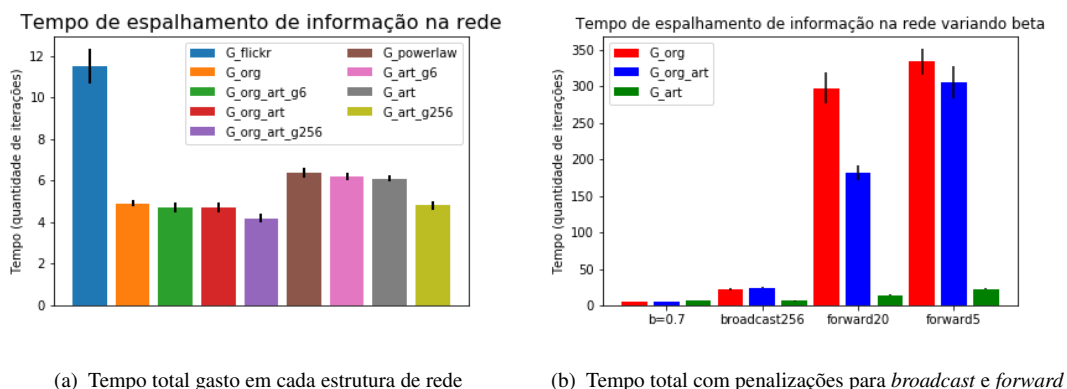


Figura 5. Tempo total exigido para contaminar toda a rede durante a simulação.

pos houve um aumento considerável no tempo, devido a maior quantidade de usuários com grau menor que 20 mas ainda maior ou igual a 5. Esses resultados sugerem que o limite de *forward* consegue afetar a viralização dos usuários, porém, variar esse limite pode ter pouco impacto, principalmente considerando os grupos artificiais, onde usuários conseguem alcançar várias pessoas com uma única mensagem.

## 5. Conclusão

Neste trabalho definimos e analisamos duas formas distintas de criação de grupos na rede do *WhatsApp*: grupos orgânicos, que dependem da topologia estrutural da rede e apresentam uma proximidade natural entre seus membros; e grupos artificiais, que são formados através de um *link* publicamente acessível com funções de divulgação de conteúdo ou interesses amplos da sociedade que incluem fatores mais externos à rede. Com isso conseguimos apontar e diferenciar formas bem distintas e conflitantes do uso do aplicativo em que uma é particular e precisa de segurança, e outra de uso em massa que possui capacidade de viralização e pode precisar de certa regulação de conteúdo. Nossa metodologia também propõe formas específicas para se gerar uma rede com características de cada tipo e construídos, respectivamente, a partir de detecção de comunidades locais e distribuições de dados reais do *WhatsApp*.

Com esse trabalho, criamos um modelo específico capaz de gerar redes heterogêneas que se assemelham à estrutura vista no *WhatsApp*, permitindo análises mais completas para essa mídia social que modelos generativos tradicionais podem não ser capazes de captar e, finalmente, utilizamos a rede proposta para aplicar um modelo epidêmico estocástico para investigar os fatores que estão por trás da propagação de informação (por exemplo, notícias falsas) em uma rede social que contenha um mecanismo de criação de grupos como a do *WhatsApp*. Nós nos concentramos em analisar a capacidade de viralização a partir da aplicação do modelo epidemiológico SI avaliando a velocidade com que um usuário “infectado” repassa essa informação para seus vizinhos. Além disso, incorporamos uma métrica de penalizações de acordo com os limites de compartilhamento, *broadcasting* e *forwarding*, determinados pelo *WhatsApp*. Dentre nossas principais descobertas, nós mostramos que penalizações no *forward* e no *broadcast* conseguem apenas atrasar o espalhamento de informação nessa rede, mas não impedem que conteúdo criptografado se espalhe de forma viral e anônima no *WhatsApp*.

## 6. Agradecimentos

Esse trabalho é parcialmente financiado por CNPq, CAPES e Fapemig.

## Referências

- Andreou, A., Silva, M., Benevenuto, F., Goga, O., Loiseau, P., and Mislove, A. (2019). Measuring the Facebook Advertising Ecosystem. In *Proc. of the Network and Distributed System Security Symposium, NDSS'19*, San Diego, CA.
- Barabási, A.-L. et al. (2016). *Network science*. Cambridge university press.
- Bessi, A. and Ferrara, E. (2016). Social Bots Distort the 2016 U.S. Presidential Election Online Discussion. *First Monday*, 21(11).
- Cha, M., Benevenuto, F., Ahn, Y.-Y., and Gummadi, K. P. (2012). Delayed Information Cascades in Flickr: Measurement, Analysis, and Modeling. *Computer Networks*, 56(3):1066–1076.
- Chakrabarti, S., Stengel, L., and Solanki, S. (2018). Duty, Identity, Credibility: 'Fake News' and the Ordinary Citizen in India. BBC World Service Audiences Research.
- Feng, Z., Li, Y., Jin, L., and Feng, L. (2015). A Cluster-Based Epidemic Model for Retweeting Trend Prediction on Micro-blog. In *Proc. of 26th Int'l Conf. on Database and Expert Systems Applications*, DEXA, Valencia, Spain.
- Freitas, C., Benevenuto, F., Ghosh, S., and Veloso, A. (2015). Reverse Engineering Socialbot Infiltration Strategies in Twitter. In *Proc. of the 2015 IEEEACM Int'l Conf. on Advances in Social Networks Analysis and Mining*, ASONAM '15.
- Garimella, K. and Tyson, G. (2018). Whatapp doc? A first look at whatsapp public group data. In *Proc. of 12th Int'l Conf. on Web and Social Media*, ICWSM'18, Stanford, USA.
- Guha, R., Kumar, R., Raghavan, P., and Tomkins, A. (2004). Propagation of trust and distrust. In *Proc. of 13th Int'l Conf. on World Wide Web*, WWW'04, New York, USA.
- Howard, P. N. and Hussain, M. M. (2011). The Upheavals in Egypt and Tunisia: The Role of Digital Media. *Journal of Democracy*, 22(3):35–48.
- Keeling, M. J. and Eames, K. T. (2005). Networks and Epidemic Models. *Journal of The Royal Society Interface*, 2(4):295–307.
- Khurana, P. and Kumar, D. (2018). Sir Model for Fake News Spreading Through Whatsapp. In *Proc. of 3rd Int'l Conf. on Internet of Things and Connected Technologies*, ICIoTCT, India.
- Malka, V., Ariel, Y., and Avidar, R. (2015). Fighting, worrying and sharing: Operation 'Protective Edge' as the first WhatsApp War. *Media, War & Conflict*, 8(3):329–344.
- McAuley, J. and Leskovec, J. (2012). Image Labeling on a Network: Using Social-Network Metadata for Image Classification. In *12th European Conf. on Computer Vision*, ECCV12, Florence, Italy.
- Melo, P., Messias, J., Resende, G., Garimella, K., Almeida, J., and Benevenuto, F. (2019). Whatsapp Monitor: A Fact-checking System for WhatsApp. In *Proc. of 13th Int'l Conf. on Web and Social Media*, ICWSM'19, Munich, Germany.
- Mondal, M., Silva, L. A. A., and Benevenuto, F. (2017). A Measurement Study of Hate Speech in Social Media. In *Proc. of ACM Conference on Hypertext and Social Media*, HT'17, Prague, Czech Republic.

- Moreno, A., Garrison, P., and Bhat, K. (2017). Whatsapp for Monitoring and Response During Critical Events: Aggie in the Ghana 2016 Election. In *Proc. of 14th Int'l Conf. on Information Systems for Crisis Response and Management, ISCRAM'17*, Albi, France.
- Radcliffe, D. and Lam, A. (2018). Social Media in the Middle East: The Story of 2017. *SSRN Electronic Journal*.
- Reis, J. C. S., Correia, A., Murai, F., Veloso, A., and Benevenuto, F. (2019). Supervised Learning for Fake News Detection. *IEEE Intelligent Systems*, 34(2).
- Resende, G., Melo, P., Sousa, H., Messias, J., Vasconcelos, M., Almeida, J., and Benevenuto, F. (2019). (Mis)Information Dissemination in WhatsApp: Gathering, Analyzing and Countermeasures. In *Proc. of the Web Conference, WWW '19*, San Francisco, USA.
- Resende, G., Messias, J., Silva, M., Almeida, J., Vasconcelos, M., and Benevenuto, F. (2018). A System for Monitoring Public Political Groups in WhatsApp. In *Proc. of the 24th Brazilian Symposium on Multimedia and the Web, WebMedia '18*, Salvador, Brazil. ACM.
- Ribeiro, F. N., Saha, K., Babaei, M., Henrique, L., Messias, J., Benevenuto, F., Goga, O., Gummadi, K. P., and Redmiles, E. M. (2019). On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook. In *Proc. of the ACM Conf. on Fairness, Accountability, and Transparency, FAT\*'19*, Atlanta, USA.
- Rosenfeld, A., Sina, S., Sarne, D., Avidov, O., and Kraus, S. (2018). A Study of WhatsApp Usage Patterns and Prediction Models without Message Content. *arXiv preprint arXiv:1802.03393*.
- Seufert, M., Hoßfeld, T., Schwind, A., Burger, V., and Tran-Gia, P. (2016). Group-based Communication in WhatsApp. In *IFIP Networking Conference and Workshops, NETWORKING 2016*, Vienna, Austria.
- Seufert, M., Schwind, A., Hoßfeld, T., and Tran-Gia, P. (2015). Analysis of Group-Based Communication in WhatsApp. In *Proc. of 7th EAI Int'l Conf. on Mobile Networks and Management, MONAMI'15*, Santander, Spain.
- Speicher, T., Ali, M., Venkatadri, G., Ribeiro, F. N., Arvanitakis, G., Benevenuto, F., Gummadi, K. P., Loiseau, P., and Mislove, A. (2018). On the Potential for Discrimination in Online Targeted Advertising. In *Proc. of the ACM Conf. on Fairness, Accountability, and Transparency, FAT\*'18*.
- Starbird, K., Arif, A., Wilson, T., Van Koevering, K., Yefimova, K., and Scarnecchia, D. (2018). Ecosystem or Echo-System? Exploring Content Sharing across Alternative Media Domains. In *Proc. of 12th Int'l Conf. on Web and Social Media, ICWSM'18*, Stanford, USA.