NDI

Análise de Dados para o Monitoramento de Redes Sociais

Tutorial sobre Técnicas, Ferramentas e Metodologias de Monitoramento e Análise de Redes Sociais

Maio 2020

NDI.ORG

Índice

AUTORES 3

SOBRE O NDI 3

AGRADECIMENTOS 4

INTRODUÇÃO 5

CONTEXTUALIZAÇÃO 6

TRABALHANDO COM COLETA DE DADOS 8

ANÁLISE DE DADOS E REDES 13

IDENTIFICANDO INFLUENCIADORES, GRUPOS E CONTAS 20

ANALISANDO CONTAS E CONTEÚDO 25

CONCLUSÃO 31

APÊNDICE I: EXEMPLO DE CÓDIGO DE API - COLETANDO DADOS NAS APIS SEARCH E STREAMING DO TWITTER COM O PACOTE RTWEET 32

APÊNDICE II: FERRAMENTAS PARA OSINT 34

REFERÊNCIAS 35

Autores

Nick Monaco é Diretor do Laboratório de Inteligência Digital do Instituto para o Futuro (Digital Intelligence Lab - Institute for the Future, ou DigIntel). Ele é especialista em desinformação *online* e na utilização de *bots* políticos, com enfoque em desinformação chinesa. Ao longo da carreira, ele manteve contato com formuladores de política e tecnólogos dos setores público e privado para se antenar sobre as melhores práticas no combate à desinformação e na proteção da integridade de eleições ao redor do mundo. Ele já havia trabalhado com esses temas na Graphika, uma empresa de análise de redes sociais e inteligência contra ameaças, e no Jigsaw, o *think-tank* de direitos digitais do Google. Ele também é pesquisador-associado do Projeto de Propaganda Computacional do Instituto de Estudos da Internet da Universidade de Oxford (Computational Propaganda Project - Oxford Internet Institute, ou ComProp).

Daniel Arnaudo é Consultor do NDI para Estratégias Informacionais, dedicado à interseção entre democracia e tecnologia, particularmente ao desenvolvimento de programas destinados ao rastreamento de desinformação e ao fomento da integridade da informação em todo o mundo. Ele também atua como pesquisador-adjunto (*fellow*) em Cibersegurança da Faculdade de Estudos Internacionais Henry M. Jackson, pertencente à Universidade de Washington (Jackson School of International Studies - University of Washington), onde participou de projetos no Brasil, em Myanmar e nos EUA. Recentemente, ele também foi colaborador do grupo de pesquisa em Propaganda Computacional do Instituto de Estudos da Internet da Universidade de Oxford (ComProp). Sua pesquisa têm como foco campanhas políticas *online*, direitos digitais, cibersegurança e tecnologias de informação e comunicação (TICs) para o desenvolvimento.

Sobre o NDI

O National Democratic Institute (NDI) é uma organização não governamental apartidária e sem fins lucrativos que responde às aspirações de pessoas de todo o mundo que almejam viver em sociedades democráticas que reconheçam e promovam os direitos humanos básicos.

Desde sua fundação em 1983, o NDI, em conjunto com seus parceiros locais, vem se dedicando ao apoio e à consolidação de instituições e práticas democráticas por meio do fortalecimento de partidos políticos, organizações da sociedade civil e parlamentos, da salvaguarda de eleições e do fomento à participação civil, à abertura e à prestação de contas em governos.

Com funcionários e ativistas políticos voluntários espalhados por mais de cem países, o NDI reúne indivíduos e grupos visando ao compartilhamento de ideias, conhecimento, experiências e competências. Disponibilizamos aos nossos parceiros um leque de informações sobre as melhores práticas do desenvolvimento democrático internacional, adaptáveis às necessidades de cada país. O enfoque multinacional do NDI corrobora a mensagem de que, embora não exista um único modelo democrático, determinados princípios fundamentais são partilhados por todas as democracias.

O trabalho do Instituto está ancorado nos princípios consagrados na Declaração Universal dos Direitos Humanos. O Instituto também tem como missão fomentar o desenvolvimento de meios de comunicação institucionalizados entre cidadãos, instituições políticas e representantes eleitos, fortalecendo capacidades para a melhoria da qualidade de vida de toda a população. Para mais informações sobre o NDI, por favor, acesse www.ndi.org.

Agradecimentos

O Instituto gostaria de expressar toda a gratidão ao National Endowment for Democracy (NED) pelo apoio na confecção deste guia. O NED é uma fundação privada sem fins lucrativos dedicada à proliferação e ao fortalecimento de instituições democráticas ao redor do mundo. A instituição financia, anualmente, mais de 1.600 projetos concebidos por organizações não governamentais empenhadas na consolidação da democracia em mais de 90 países. Desde que foi fundado, em 1983, o NED se manteve na vanguarda das lutas por democracia mundo afora e se transformou num polo multifacetado de atividades, recursos e intercâmbio intelectual para ativistas, profissionais e acadêmicos de todo o mundo ligados ao tema da democracia.

O NDI também gostaria de agradecer ao Instituto para o Futuro (Institute for the Future ou IFTF) pela cooperação e pela parceria na distribuição do guia. O IFTF é uma organização sem fins lucrativos dedicada ao futuro da sociedade civil e é a principal instituição mundial de futurologia. Há mais de 50 anos, empresas, governos e organizações de impacto social vêm contando com as previsões internacionais, as pesquisas customizadas e os programas de capacitação em análise prospectiva (*foresight*) realizados pelo IFTF para se guiar frente a mudanças complexas e desenvolver estratégias à altura dos desafios globais. O IFTF oferece metodologias e ferramentas que proporcionam perspectivas coerentes de transformação em todos os setores que somam forças na batalha por um futuro mais sustentável.

Design e Impressão: Ironmark, 2020

Introdução

As redes sociais vêm ganhando cada vez mais relevância na interlocução entre cidadãos, candidatos, partidos e organizações afins para a articulação de eventos políticos, eleições, referendos, votações em projetos de lei, greves e outras formas de ativismo político. Nesse sentido, é fundamental que pesquisadores, observadores eleitorais, organizações da sociedade civil e a população em geral estejam munidos de ferramentas, métodos e práticas que contribuam para a coleta e a análise de dados do espaço virtual. Integrantes de organizações da sociedade civil internacionais, incluindo pesquisadores, gestores de projeto e ativistas, vêm se engajando em diversos programas internacionais, como missões de observação eleitoral, com o objetivo de auxiliar grupos locais a desenvolverem a própria capacidade de monitoramento, ou o monitoramento de discursos de ódio, tendências políticas e outros temas.

Este guia tem como objetivo apresentar a pesquisadores, observadores eleitorais, tecnólogos e outros atores sociais as práticas, as ferramentas e as metodologias mais indicadas para a análise e o monitoramento de redes sociais. Introduziremos os conceitos mais relevantes a serem assimilados nesses tipos de pesquisa e examinaremos como traçar um quadro abrangente do contexto sociotécnico de um país ou de uma região, o que inclui conhecer a presença *online* dos partidos políticos locais, o grau de penetração da internet e das redes sociais, o cenário midiático, divisões étnicas e religiosas e diversos outros fatores reproduzidos no espaço virtual.

Abaixo, os principais tópicos abordados ao longo deste ensaio:

- **Colaboração:** É importante que pesquisadores considerem parcerias em potencial e formas de articulá-las, seja com diferentes tipos de associações locais ou ONGs internacionais dedicadas ao tema ou com um rol de instituições de mercado que vão desde microempresas especializadas a grandes multinacionais que controlam as plataformas de mídia social e outras tecnologias de alcance global. Possibilidades de colaboração serão examinadas e ponderadas numa seção à parte, contendo exemplos e um balanço dos riscos e benefícios envolvidos em múltiplas parcerias.
- **Metodologia:** No que tange à metodologia, examinaremos métodos distintos para a coleta de dados, trazendo ponderações sobre as diferentes plataformas e suas respectivas APIs, assim com as opções de raspagem de conteúdo.
- **Mapeamento e Visualização:** Uma seção será dedicada à elaboração e à interpretação de mapas de redes sociais. Apresentaremos os principais termos técnicos, além de métodos para o desenvolvimento de mapas do ciberespaço, exemplos de pesquisa de campo e possíveis limitações dos mapas.
- **Análise:** Nessa seção, examinaremos o conjunto de entidades e indivíduos que moldam o debate a partir de um panorama geral sobre o papel exercido por contas, influenciadores e grupos específicos no ecossistema virtual e de uma avaliação sobre as formas de protagonismo de veículos de notícia e de outras fontes externas na disseminação de conteúdo.
- **Conteúdo:** O conteúdo publicado na internet será abordado no guia a partir das diferentes características de postagens e *tweets* e de outros tipos de rede social. Demonstraremos como detectar diferentes tipos de propaganda computacional em rede, como *botnets*, fábricas de *trolls* e outras formas de manipulação, considerando os diversos tipos de conteúdo malicioso, como desinformação e discurso de ódio, bem como os alvos em potencial.
- **Ferramentas:** Para dar suporte às técnicas de investigação apontadas no guia, foram catalogadas e examinadas diferentes ferramentas propícias ao desenvolvimento de análises distintas relativas ao monitoramento de redes sociais, incluindo instrumentos para a coleta de dados em plataformas distintas e recursos para análise de redes, visualização de dados e pesquisas de inteligência de fontes abertas.
- **Desfechos:** Por último, serão examinados os possíveis desfechos alimentados e realçados com base nas análises, como a captura de dados para pesquisa, o trabalho de documentação e a elaboração de mecanismos de denúncia junto às plataformas, aos órgãos reguladores e às organizações de monitoramento eleitoral. O final do guia contém recomendações para o desenvolvimento de pesquisas em áreas a serem exploradas futuramente e de avaliações críticas sobre as áreas em evolução.

Contextualização

Diante de novos contextos, analistas devem levar em conta os sistemas técnicos e os múltiplos atores, redes e grupos sociopolíticos envolvidos, avaliando diversos aspectos do cenário informacional, social e político local, incluindo as redes e a estrutura do país e da região e sua posição no sistema global. Informações nem sempre circulam por meio de redes de notícia *online* ou tradicionais; grande parte é transmitida de boca em boca, através de boatos, da mídia tradicional ou por outros meios, modalidades que são cada vez mais praticadas na internet, onde podem ser mais facilmente mapeadas e analisadas.

Muitas organizações ao redor do mundo empregam táticas destinadas a manipular a percepção do público sobre candidatos e temas, a minar a confiança no processo democrático e a confundir o eleitorado sobre locais de votação, cadastramento e o próprio sistema eleitoral. Um dos principais objetivos de pesquisas como esta é contribuir para desvendar como as redes de propaganda computacional[1] operam no ciberespaço, ajudando a expor como elas funcionam, documentar casos para pesquisa e, possivelmente, alertar autoridades ou empresas de mídia social sobre manipulações ou violações na internet. A detecção de automações, contas falsas, conteúdo falso, fontes de informação duvidosas e outras formas de manipulação faz parte desse esforço de caracterização das diferentes nuances da propaganda computacional.

Analistas de redes sociais que buscam informações em diferentes contextos internacionais devem levar diversos fatores em consideração na elaboração do relatório de dados, aplicando ferramentas, pesquisando sobre o ambiente normativo e institucional do espaço informacional específico e empregando métodos *offline*—como entrevistas com autoridades do governo, partidos, meios de comunicação e candidatos—para tentar apreender, ao máximo, o cenário de desinformação em meio à eleição trabalhada.

"Desinformação" é um conceito de difícil assimilação por ser um termo sem uma definição muito precisa. Um dos fatores que caracterizam o conceito é a ideia de intencionalidade: a desinformação é transmitida com a intenção de ludibriar, enquanto a má informação (*misinformation*) refere-se a conteúdos imprecisos transmitidos sem a intenção de distorcer a realidade. Para saber mais sobre questões semânticas e se aprofundar no assunto, acesse o léxico de mentiras elaborado pela *Data & Society* (intitulado *Lexicon of Lies*) e o relatório sobre desordem informacional da *First Draft*, além do guia desenvolvido pelo NDI em defesa da integridade da informação e do discurso político civil [2], que conta com traduções em albanês, árabe, inglês, francês, russo, sérvio e espanhol. As demais fontes estão descritas na seção de referências bibliográficas.

Também é importante considerar, na análise, outros tipos de conteúdo inofensivos, maliciosos ou positivos para além da desinformação, assim como o papel da mídia local e as formas de introjeção e influência dos meios de comunicação na internet e nas redes sociais. Procure explorar os principais jornais impressos, radiofônicos e televisivos, avaliando o peso de cada um no mercado, os vínculos com partidos políticos, governos e empresas e as estratégias de influência digital. Muitos veículos tradicionais ocupam um espaço considerável no meio virtual e, especialmente quando associados a um partido político relevante, podem exercer enorme influência na linha editorial e nas preferências políticas de uma organização, além de servirem como indutores - orgânicos ou artificiais - de viralização. No contexto das redes, a polarização ganha outra dimensão, tornando-se facilmente perceptível a formação de grupos mais amplos e diversificados favoráveis ou contrários a determinada pauta, o que também pode sinalizar níveis presentes de propaganda computacional e desinformação.

Discursos de ódio geralmente contêm desinformações destinadas a difamar alvos de campanhas por meio de ataques falsos, atingindo especialmente mulheres, minorias e demais grupos vulneráveis. A pesquisa sobre violência contra mulheres na política[3] realizada pelo grupo de trabalho sobre Gênero, Mulheres e Democracia do NDI salienta que, "quando ataques contra mulheres politicamente ativas são canalizados na internet, o caráter expansivo das plataformas sociais amplia os efeitos do assédio psicológico por meio do anonimato, da ausência de fronteiras e da reiteração, comprometendo a sensação de segurança pessoal das mulheres de formas não partilhadas por homens. Grande parte dos atores estatais e não-estatais que cometem atos de violência *online* contra mulheres na política tende a se mobilizar em redes transnacionais. O uso indevido —perpetrado por Estados, organizações e indivíduos— de liberdades supostamente propiciadas pelo universo informacional se tornou uma das principais ameaças à integridade da informação." (Zeiter et al., 2019, 4) Como consequência, é importante que pesquisadores estejam atentos à vulnerabilidade particularmente de mulheres a ataques virtuais, ponderando formas de documentar e denunciar às plataformas violações dessa natureza. O NDI tem tomado a dianteira no uso de léxicos de termos ligados a

1 Segundo o Instituto de Estudos da Internet da Universidade de Oxford (*Oxford Internet Institute*), cujo grupo de pesquisa contribuiu para definir o termo e inaugurou grande parte das pesquisas relacionadas ao tema, "propaganda computacional representa o uso de algoritmos, automação e curadoria humana com o objetivo de distribuir propositadamente informações falaciosas em redes sociais " (Woolley e Howard, 2017, 4).

2 Cujo título em inglês é "*Supporting Information Integrity and Civil Political Discourse*". Disponível em: https://www.ndi.org/publications/supporting-information-integrity-and-civil-political-discourse

3 Denominada, em inglês, "*Violence Against Women in Politics*" ou "VAW-P".

discursos de ódio em pesquisas sobre redes sociais, com estudos de caso realizados na Colômbia, na Indonésia e no Quênia. Os métodos para a elaboração dos léxicos e os estudos de caso podem ser consultados em detalhe no relatório resultante da pesquisa, intitulado "*Tweets that Chill: Analyzing Violence Against Women in Politics*[4]".

Estratégias para a coleta de dados devem ter em conta a forma como procedimentos informacionais baseados em discurso de ódio e propaganda computacional operam nos contextos analisados. Ao longo deste guia, analistas terão a oportunidade de aprender como identificar campanhas, redes e usuários, mas é essencial que pesquisadores estejam bem familiarizados com os tipos de propaganda computacional e conteúdo nocivo existentes e outros padrões que tendem a aparecer durante a pesquisa.

É igualmente recomendável possuir um amplo conhecimento sobre o contexto regulatório (o que inclui a regulamentação de eleições e financiamentos de campanha, que pode ajudar a embasar denúncias) e sobre as regras de moderação de conteúdo e as políticas que regem as plataformas, contribuindo para que pesquisadores desenvolvam estratégias de pesquisa amparadas na lei e na ética, alertem empresas—e potencialmente governos—sobre assédios e outras condutas ilegais e maliciosas praticadas na internet e compreendam melhor os países analisados.

Um aspecto crucial para a realização de denúncias é ter conhecimento sobre os termos de serviço das diferentes empresas de mídia social. A seguir, estão listados os principais critérios adotados pelas plataformas Facebook, Twitter e YouTube, com os respectivos *links* para as políticas.

Padrões da Comunidade do Facebook	▪ Informações relevantes sobre denúncias em circunstâncias distintas, aqui. ▪ "Denunciar uma Página Impostora de uma Figura Pública," aqui. ▪ "Como Denunciar Algo," desagregado por diferentes tipos de postagem, aqui. ▪ "Como faço para marcar uma publicação do Facebook como notícia falsa?", aqui.
Regras do Twitter	▪ Visão geral sobre denúncias de violações, aqui. ▪ Como denunciar um tweet, uma conta abusiva ou uma mensagem individual, aqui. ▪ Denunciando contas de falsa identidade, aqui. ▪ Instruções para denúncias de spam, aqui.
Diretrizes da Comunidade do YouTube	▪ Como denunciar conteúdos inapropriados, desagregado por tipo de postagem, aqui. ▪ "Denunciar uma previsão de pesquisa do YouTube," aqui. ▪ "Outras opções de denúncia," aqui. ▪ "Como denunciar um spam ou conteúdo enganoso," aqui (final da página). ▪ Mecanismo de denúncia do YouTube, aqui.

Algumas empresas, como o Facebook, exigem que o usuário se identifique com informações verdadeiras. Então o simples reconhecimento de uma conta pertencente a uma pessoa fictícia, ou a um grupo ligado a uma conta falsa, pode levar ao encerramento da conta. Outras empresas, como o Twitter, não proíbem o anonimato, embora imponham restrições a discursos de ódio e amplificações artificiais, que podem ser extraídos por meio de pesquisas. Vale a pena se familiarizar com a variedade de códigos e mecanismos destinados a denúncias de conteúdo, como os esboçados na tabela acima.

Denunciar é importante, assim como documentar campanhas, contas e postagens relevantes para a checagem das denúncias. Opte por sistemas que podem ser facilmente reproduzidos e consultados, em termos de comentários e fluxos de trabalho. Como mencionado acima, nos Padrões da Comunidade do Facebook, estão disponibilizados mecanismos para denunciar contas falsas e conteúdo mal-intencionado e solicitar a checagem e a possível remoção de conteúdos considerados nocivos. O Twitter permite diferentes tipos de denúncia a identidades falsas, spams e determinados discursos proibidos ou de ódio. As diretrizes do Youtube focam mais em meios de comunicação e direitos autorais, assim como em manifestações explícitas, de ódio e outros tipos de conteúdo nocivo. Os termos de referência do Google, controlador do YouTube, explicitam como, além de denunciar contas, é possível investigar contas vinculadas à plataforma de *streaming*.

Em termos de normas governamentais, analistas devem se atentar às leis de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados da União Europeia, que abrange a coleta de informações de identificação pessoal de cidadãos da

4 Em tradução livre, "*Tweets* de Arrepiar: Analisando a Violência contra Mulheres na Política".

União Europeia por parte de organizações operando ou não no espaço comum europeu.[5] A coleta de dados de redes, grupos e usuários privados pode ter um efeito revogatório sobre essas leis e os termos de serviço das plataformas.

Redes como a Design 4 Democracy Coalition [6] (D4D Coalition) podem contribuir para o fomento de princípios democráticos em empresas de tecnologia ––por exemplo, chamando a atenção das plataformas para grandes campanhas de influência associadas a propaganda eleitoral, discursos de ódio e outros propósitos. A rede D4D Coalition consiste na articulação entre organizações da sociedade civil nacionais e internacionais com empresas de tecnologia visando à incorporação e à defesa de princípios democráticos, incluindo na moderação de conteúdo, na formulação de políticas e em questões de produto. A rede conecta membros da sociedade civil e do movimento de luta pela democracia oriundos de diferentes contextos a algumas das mais influentes empresas de tecnologia (como Facebook, Microsoft e Twitter) com o objetivo de compartilhar informações e desenvolver estratégias destinadas à promoção da integridade das informações e à salvaguarda de processos democráticos. Iniciativas como esta podem ser apoiadas e realçadas por meio de documentações, análises e denúncias baseadas nas ferramentas, nos métodos e nas táticas apresentadas neste guia.

Para mais informações sobre o desenvolvimento de estratégias para a análise de dados de redes sociais em eleições, consulte as orientações do NDI sobre desinformação e integridade de eleições[7] e o guia elaborado pelo programa Supporting Democracy para o monitoramento de redes sociais em eleições a partir da sociedade civil (*Guide for Civil Society on Monitoring Social Media for Elections*)[8]. Os dois guias contêm metodologias e considerações normativas para observadores no que tange ao monitoramento de redes sociais e à possibilidade de incorporação de dados coletados *online* em missões de observação eleitoral tradicionais.

Trabalhando com Coleta de Dados

A coleta de dados é a primeira etapa para uma análise criteriosa de atividades *online* em meio a uma eleição. O primeiro passo do analista que almeja trabalhar in loco é fazer uma sondagem do panorama dos meios de comunicação *online* e das redes sociais na localidade analisada. Eis algumas perguntas importantes a serem consideradas:

- **Quais são as plataformas mais populares na região analisada? Qual é o grau de penetração de cada plataforma?** O Internet World Stats (portal de estatísticas mundiais), a União Internacional de Telecomunicações, o relatório anual sobre liberdade na internet elaborado pela Freedom House (*Freedom on the Net*) ou o próprio Facebook são boas fontes de consulta. Por exemplo, em um país com alto grau de penetração do Facebook e baixo grau de penetração do Twitter (como Taiwan), o Facebook é provavelmente a rede social que mais tende a gerar *insights*.
- **Quais são os portais de notícia mais populares na localidade? Quais destes pertencem a veículos de imprensa tradicionais e quais foram criados mais recentemente?**
- **Quais são as hashtags mais relevantes na eleição em questão? Do mesmo modo, quais contas oficiais representam partidos, candidatos e suas respectivas campanhas na eleição?** Muitas vezes, um candidato possui mais de uma conta ou página eleitoralmente relevante - como uma conta pessoal e uma conta oficial da campanha no Twitter. Um bom ponto de partida para a captura dos dados mais valiosos é listar essas contas.

Uma vez identificados os portais e as plataformas de mídia social mais importantes do país analisado, já é possível dar início à coleta de dados. Nesta seção, examinaremos as opções à disposição dos pesquisadores para a realização da coleta.

5 https://gdpr.eu/

6 Coalisão para o desenvolvimento de tecnologias dedicadas à causa democrática, coordenada pelo NDI, pelo Instituto Internacional Republicano (International Republican Institute), pela Fundação Internacional para Sistemas Eleitorais (International Foundation for Electoral Systems) e pelo Instituto Internacional para Democracia e Assistência Eleitoral (International IDEA).

7 https://www.ndi.org/publications/disinformation-and-electoral-integrity-guidance-document-ndi-elections-programs

8 Supporting Democracy é uma iniciativa implementada por um consórcio composto por SOFRECO, Democracy Reporting International (DRI) e NDI. https://democracy-reporting.org/wp-content/uploads/2019/10/social-media-DEF.pdf

Métodos para a Coleta de Dados

Pesquisadores têm à disposição diversas opções para a coleta de dados de redes sociais. Os três principais recursos são a utilização de ferramentas para a coleta de dados de terceiros, a comunicação direta com as APIs das plataformas ou a técnica de *web scraping*. A seguir, vamos nos aprofundar em cada um dos três métodos, salientando as diferenças entre eles.

Coleta de Dados de Terceiros (Acesso Indireto)

Para pesquisadores com a agenda apertada ou sem conhecimento para interagir com sites por código, uma boa opção são ferramentas para coletar dados de terceiros. Normalmente, essas ferramentas viabilizam o acesso em segundo plano a APIs de uma ou mais plataformas e exibem os dados capturados de um modo inteligível e gráfico por meio, por exemplo, de um *dashboard*. No caso do Facebook, que, atualmente, não permite que pesquisadores ou empresas externas utilizem sua API, uma das opções mais recomendadas para monitorar o alcance de páginas, grupos ou URLs é a ferramenta CrowdTangle, também utilizada para mensurar o alcance de URLs nas plataformas Twitter, Instagram e Reddit. A extensão do CrowdTangle [9] para o Google Chrome permite que o usuário visualize em tempo real uma estimativa do número de reações a postagens, páginas ou URLs, o que pode ser útil para monitorar diariamente os conteúdos que estão mais em voga nas diferentes plataformas.

Embora determinadas ferramentas utilizadas para a coleta de dados de terceiros, como Sysomos e Brandwatch, exijam assinaturas com custo relativamente elevado, elas dão acesso a grandes quantidades de dados, o que pode ser profícuo para o monitoramento de campanhas via *hashtag* e de outros tópicos em voga nas redes sociais.

Geralmente, os dados coletados por meio dessas ferramentas podem ser visualizados em um navegador e exportados para um arquivo legível por máquina, como em formato CSV (*Comma Separated Values* ou "valores separados por vírgula"), que, por sua vez, pode ser manipulado por um cientista de dados para que os dados possam ser tratados.

Facebook: Sysomos, Brandwatch
Twitter: Twitonomy

Acesso Direto - APIs e Web Scraping: Qual é a diferença?

Para interações mais diretas com plataformas e sites, pesquisadores podem utilizar uma Interface de Programação de Aplicações (*Application Program Interface* ou API) ou então coletar a informação diretamente do código-fonte do site, técnica conhecida como "*web scraping*" ("raspagem de dados").

É importante assinalar a diferença entre os dois métodos: na maioria dos casos, APIs são meios legítimos e éticos de capturar dados, já que estes são regulamentados pelas próprias plataformas e compartilhados sem que haja violação de direitos autorais; já o método de *web scraping* costuma envolver violações de Termos de Serviço e é mais difícil de ser regulamentado, sendo, muitas vezes, uma prática ilegal. É comum que pesquisadores se refiram, incorretamente, à captura de dados via APIs como "raspagem" de dados. É importante saber a distinção entre os dois métodos, não só por razões utilitárias, como poupar tempo e esforço, mas também devido às possíveis violações éticas e legais associadas a práticas de *web scraping*.

Uma vez salientada a diferença entre as duas abordagens, agora vamos nos aprofundar em cada uma delas.

APIs

Pesquisadores interessados em uma abordagem mais objetiva podem acessar diretamente os dados via interfaces de programação de aplicações (APIs), disponibilizadas por diversas plataformas. De um modo geral, essa é uma maneira relativamente simples de interagir com um site ou uma plataforma de mídia social por código, o que possibilita que usuários processem rapidamente uma quantidade muito maior de dados do que seria possível manualmente, gerando análises muito mais contundentes das atividades *online*.

9 Atualmente, o CrowdTangle está disponível para acadêmicos e pesquisadores de forma seletiva, mediante solicitação no site CrowdTangle.com. A versão completa do CrowdTangle inclui dados atuais e históricos do Facebook e do Instagram. No site, também é possível encontrar uma extensão gratuita da ferramenta que permite, a partir de consultas a URLs específicas, a visualização das 500 postagens públicas de ampla repercussão mais recentes nas plataformas Facebook, Instagram, Reddit e Twitter. Tanto a versão completa quanto a extensão podem ser úteis para a realização de pesquisas.

Tipos de API

Antes de iniciar a coleta de dados, dois fatores particularmente relevantes para se atentar em relação às APIs são a acessibilidade e a divisão cronológica dos dados.

- **Acessibilidade:** APIs podem ser abertas, ou seja, acessíveis a qualquer usuário, ou sujeitas à autenticação, isto é, quando o acesso aos dados só é permitido mediante alguma forma de certificação do usuário.
  - **APIs Abertas:** O Venmo, um aplicativo utilizado para a realização de pagamentos eletrônicos nos EUA, possui uma API pública que permite que qualquer usuário visualize um número determinado de transações mais recentes processadas no aplicativo. A internet está repleta de listas de APIs abertas - como a elaborada pelo GitHub. O portal Any-api.com também disponibiliza a usuários interessados uma lista com diversas APIs públicas, muitas delas abertas.
  - **APIs Sujeitas à Autenticação:** A maioria das APIs acessadas para a captura de dados de redes sociais (Twitter, Reddit etc.) exige a autenticação do usuário.
- **Divisão cronológica dos dados:** Sites e plataformas também costumam organizar as próprias APIs em função de delimitações temporais.
  - **Capturando dados históricos:** A maioria das APIs permite a coleta de determinados dados antigos nos sites, como nos casos do Twitter e do Reddit. APIs destinadas à coleta de dados históricos permitem que o usuário extraia dados retroativos, gerados *anteriormente* à consulta. Mas, atenção, dados postados após a realização da consulta não podem ser coletados.
  - ***Streaming* de dados em tempo real:** O consumo e o *download* de dados em tempo real é chamado de *streaming*. Caso o Twitter seja uma plataforma relevante durante a eleição monitorada pelo analista, *streaming* talvez seja a melhor opção para a coleta de dados. Nesse caso, os *tweets* são coletados em tempo real mediante uma consulta específica (como, por exemplo, todos os *tweets* contendo a *hashtag* #eleição, ou todos os *tweets* que fazem menção a contas de interesse, URLs de interesse etc.).

Controles na Coleta de Dados via API

Com o intuito de garantir a privacidade e a segurança do usuário, a maioria das plataformas de mídia social delimita a quantidade de dados coletados individualmente. A seguir, mostraremos algumas formas de controle para que o analista possa se familiarizar com situações vivenciadas durante a coleta de dados.

- **Controle do Volume de Dados:** A maioria das APIs delimita o volume de dados coletados por usuário. Por exemplo, na extração de dados em tempo real no Twitter, cada usuário só tem direito a, no máximo, 1% do total de dados de *streaming* da plataforma.
  - **Controle da taxa de API:** Esse é o tipo mais comum de controle do volume de dados em APIs. A maioria das APIs delimita o número de solicitações realizadas para assegurar que um único usuário ou aplicação não baixe uma quantidade excessiva de dados (definida pela plataforma ou pelo site). Por exemplo, o Twitter delimita o número de *downloads* de *tweets* por usuário a cada intervalo de 15 minutos.
- **Controle dos dados removidos:** Como já pontuado, plataformas tendem a remover determinados tipos de conteúdo que violam normas e regulamentos de uso (denominados de diversas maneiras: "padrões da comunidade", "termos de serviço" etc.). Essa é uma questão particularmente importante em contextos eleitorais, marcados por condutas mal-intencionadas – na interface de *streaming* do Twitter, é possível extrair e reter dados em tempo real relativos a usuários mal-intencionados que serão potencialmente removidos e indisponibilizados pela plataforma. Se o intuito é analisar informações referentes a má condutas, desinformação e outros tipos de conteúdo numa etapa posterior, o método mais recomendável é o *streaming* de dados em tempo real.
- **Controle dos tipos de dados:** A maioria das plataformas também delimita os tipos de dados coletados por usuário. A API do Twitter permite a captura de certas informações sobre o usuário alvo (como o número de postagens, o número de seguidores e a data de criação da conta), mas proíbe o acesso a outros tipos de dados (como o endereço de IP mais utilizado pelo usuário). Atualmente, o Facebook restringe totalmente a coleta de informações sobre outros usuários ou páginas por meio de sua API. É importante estar familiarizado com os tipos de dados cuja coleta é permitida nas plataformas analisadas durante o delineamento da estratégia de pesquisa.

- **Controle de dados históricos:** O Twitter só disponibiliza na sua interface dados postados até 7 a 9 dias antes da data de coleta. Dados anteriores a 7-9 dias podem ser adquiridos por meio de provedores de dados como o GNIP, mas não podem ser coletados através do acesso padrão à API.

Um aspecto interessante das APIs é a multiplicidade de linguagens. Dados podem ser extraídos usando Java, Python, R, Ruby, Perl ou qualquer outra linguagem de programação que o analista ou sua equipe de especialistas em tecnologia optarem. Apesar disso, determinados pacotes em linguagens de programação populares simplificam o processo de consulta à API ao solucionar alguns dos entraves encontrados.

Ao final do guia, apresentamos um exemplo de código, com orientações sobre a utilização do pacote *rtweet* (em linguagem R) para a coleta de dados nas APIs Search e Streaming do Twitter (*Apêndice: Exemplo de código de API – Coletando Dados nas APIs Search e Streaming do Twitter com o Pacote Rtweet*).

Web Scraping

Embora ofereçam uma maneira eficiente de capturar dados em plataformas ou serviços, APIs não são o único método disponível. Outra opção é extrair o código-fonte de um site e minerar os dados mais relevantes, num processo chamado de *web scraping*.

Toda página na internet é constituída por um código-fonte - HTML e outros scripts, linguagens, *hyperlinks* e fontes de mídia dinâmicos -, e o procedimento realizado por um navegador de conversão de códigos em uma página visualmente acessível e interativa é chamado de *renderização*. A maioria dos navegadores utilizados atualmente - Google Chrome, Mozilla Firefox, Safari, Brave e Opera - permite a visualização do código-fonte do site. No Google Chrome, por exemplo, ao clicar com o botão direito em qualquer página carregada (ou "*renderizada*") no navegador e selecionar a opção "*Exibir Código Fonte*", será aberta uma nova janela com os códigos HTML e CSS utilizados no carregamento da página. Abaixo, um exemplo desse recurso no *yahoo.com*.

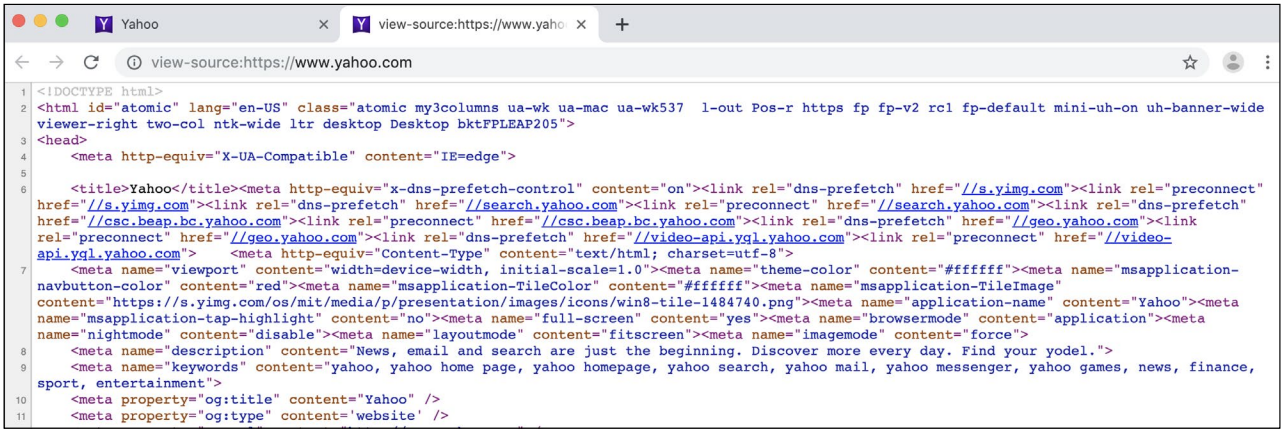


Imagem dos códigos-fonte HTML e CSS do yahoo.com *(tela capturada no início de agosto de 2019). O Google Chrome e outros navegadores modernos permitem que os usuários visualizem o código-fonte de qualquer site acessado – é o código-fonte que é extraído na "raspagem" dos dados do site.*

Considerações éticas relativas à prática de *web scraping*

Embora a técnica de *web scraping* (raspagem de dados) seja útil para a análise de páginas na internet, esse método costuma representar uma violação dos termos de serviço da maioria das plataformas de mídia social e pode, muitas vezes, incorrer em crime. Por isso, ao realizar a raspagem de dados, é sempre recomendável se ater à privacidade dos usuários, a "termos e condições" relevantes e às principais leis vigentes sobre o tema, garantindo que a coleta esteja em conformidade com os preceitos éticos e a legislação. ***É justamente pelos motivos supracitados que muitos pesquisadores se limitam a coletar dados por meio de APIs.***

Também é importante assegurar que os dados coletados por outras equipes ou ferramentas - algo frequente nesse tipo de análise - tenham sido obtidos eticamente. Por razões legais, éticas e políticas, dados raspados e hackeados ilegalmente não deveriam ser utilizados em pesquisas, que se tornam passíveis de processos por parte de governos e empresas. É importante que essas considerações sejam contempladas antes de dar início à análise dos dados.

Diferenças entre as plataformas: *Quadro-síntese*

	API para a coleta de dados históricos	API para *streaming*	Ferramentas para a coleta de dados de terceiros
Twitter	Sim	Sim	CrowdTangle (extensão)
Facebook	Não	Não	CrowdTangle
Gab	Sim, através do Pushshift.io	Não	Não
Instagram	Não	Não	CrowdTangle
Reddit	Sim	Sim (determinados pacotes possuem essa função – p.ex., Reddit SSE)	CrowdTangle (extensão) Pushshift.io
YouTube	Sim	Não	
Telegram	Sim	Não	Telethon Pushshift.io
VKontakte	Sim	Não	
WhatsApp	Sim – a interface do WhatsApp Business permite a conexão automatizada entre empresas e clientes. Não costuma ser utilizada para o tipo de análise debatido neste guia.	Não	Diversas ferramentas para a coleta de dados de terceiros propiciam análises estatísticas ou visualizações das conversas do WhatsApp[10]. ▪ ChatAnalyzer ▪ WhatsApp Chat Analyzer ▪ Chatilyzer ▪ WhatsAnalyzer

Ferramentas úteis para a coleta de dados em contextos eleitorais íntegros:

- **Pacotes para as APIs do Twitter:**
  - Pacotes em R: rtweet, twitteR
  - Pacotes em Python: python-twitter, tweepy
- **CrowdTangle** - Atualmente, o CrowdTangle e a extensão do CrowdTangle são as melhores ferramentas para a análise de dados do Facebook e do Instagram.
- **Pushshift.io** - um site que armazena dados das plataformas Reddit, Gab, Twitter e Telegram. O fundador e operador do Pushshift, Jason Baumgartner, obtém dados via APIs, tornando o uso dos dados seguro de uma perspectiva ética.
  - **Ferramenta de *streaming* de dados do Reddit:** https://github.com/pushshift/reddit_sse_stream

10 Essas ferramentas têm implicações em termos de privacidade. Particularmente em relação à análise de dados do WhatsApp, é importante garantir que conversas privadas não fiquem vulneráveis a terceiros.

- **Media Cloud (MIT)** - O Media Cloud do MIT é uma ferramenta de compilação de notícias que pode ser útil para explorar a cobertura de temas de interesse em veículos variados. Segundo as palavras dos próprios criadores no site, a ferramenta serve para "*compilarmos dados de mais de 50 mil fontes de notícia ao redor do mundo em mais de 20 línguas, incluindo espanhol, francês, hindi, chinês e japonês. Nossas ferramentas contribuem para a análise, o compartilhamento e a visualização de informações sobre assuntos tratados na mídia sob três eixos principais: picos de interesse e de cobertura dos temas, análises de redes e a utilização de línguas clusterizadas*".

Análise de Dados e Redes

O processo de elaboração de representações visuais e análises dos laços estabelecidos em redes sociais é chamado de *Análise de Redes Sociais* (ARS), também caracterizada como o desenvolvimento de mapas de redes sociais, ou o "mapeamento" de redes sociais. Embora nem sempre seja necessário para captar a cobertura midiática de determinada eleição na internet, esse tipo de análise pode ser frutífero para gerar *insights* reveladores sobre as dinâmicas de influência dentro de determinada comunidade numa rede social e visualizar os laços internos à comunidade.

O mapeamento de redes sociais consiste, fundamentalmente, em cinco etapas:

1. Coleta de dados
2. Definição das relações a serem mapeadas
3. Poda dos dados
4. Elaboração do mapa
5. Análise do mapa

Vamos explorar cada uma dessas etapas mais adiante.

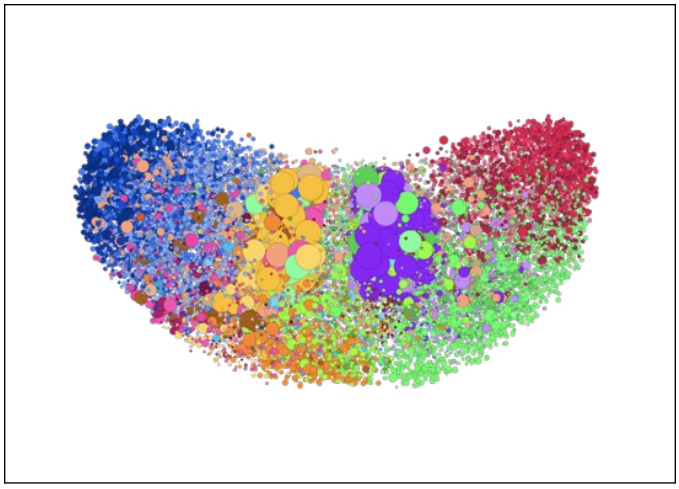
Terminologia Básica

Na hora de analisar e debater sobre ARS, é importante estar familiarizado com alguns termos para se inteirar melhor sobre a prática e o vocabulário do monitoramento de redes sociais.

Redes são extremamente úteis devido à pluralidade de relações e contextos capturados. Apesar da maior notoriedade do mapeamento de redes sociais, redes também podem ser aplicadas, por exemplo, na projeção da propagação de doenças e vírus, no mapeamento de atividades neurais no cérebro ou na reprodução de alternativas de itinerário em viagens interurbanas.

Por mais benéfica que seja, essa multifuncionalidade das redes exige a edificação de uma linguagem abstrata uniforme e universalmente aplicável. Nesta seção, introduziremos alguns termos básicos que podem ser úteis para o debate. Os mais importantes são *grafo*, *nó* e *aresta*.

- **Grafo** – *Grafo* é o termo da ciência da computação para uma rede composta por *nós* e *arestas*. É importante estar familiarizado com o termo porque é provável que ele apareça em ferramentas de mapeamento ou em fóruns de discussão. O termo *grafo* pode ser entendido praticamente como sinônimo de *rede*.
- **Nó (ou vértice)** – *Nós* são os elementos que compõem uma rede. É fundamental ter em mente que os nós possuem significados diferentes dependendo do mapa (da visualização) observado. No mapa da rede de sites pro-Kremlin desenvolvido por Lawrence Alexander, um nó representa um domínio, enquanto que, no mapa do panorama político do Twitter americano, desenvolvido pela Graphika em 2018, cada nó circular representa uma conta do Twitter.



Nesse mapa do espectro político americano em 2018 no Twitter, desenvolvido pela Graphika, é possível visualizar os nós. Cada círculo no mapa é um nó representando uma conta individual do Twitter. Nós e arestas são os dois principais componentes das redes.

- **Aresta (ou arco)** – *Arestas* são os elos entre os nós de uma rede. Geralmente representados por uma linha simples entre dois nós, esses elos podem ter diversos significados. Na modelagem do contágio de uma doença viral, por exemplo, arestas podem retratar a transmissão do vírus de um hospedeiro a outro. Em um grafo de aeroportos dos EUA, as arestas entre dois nós (aeroportos) podem significar um voo direto entre dois aeroportos da rede. Arestas podem ser direcionadas ou não-direcionadas[11] e podem conter um valor numérico associado[12] (geralmente chamado de *peso*).
  - Em grafos de redes sociais, arestas costumam representar interações por meio de "seguindo", *retweets* ou curtidas. A maioria das redes mapeadas a partir do Twitter são de *seguidores*[13] (com *arestas* indicando que um usuário segue outro) ou de *retweets*.

Mapeando uma Rede Social: Passo a Passo

Nesta seção, vamos descrever e examinar as cinco etapas envolvidas na elaboração de mapas de redes sociais, que servirão de base para uma boa interpretação dos dados.

1. **Coleta de Dados** – Como visto na última seção, essa etapa envolve a coleta de dados relevantes para uma eleição local utilizando a API de uma rede social ou alguma ferramenta de captura de dados de terceiros. Os dados coletados compõem a base de dados necessária para realizar o mapeamento da rede social. É importante ter ciência de que *somente fragmentos dos dados coletados serão utilizadas na elaboração do mapa* – a mesma base de dados pode ser utilizada no desenvolvimento de mapas diferentes. Concluída essa etapa, é hora de definir os tipos de rede/relações a serem investigadas e selecionar os dados mais relevantes.
2. **Definição das relações a serem mapeadas** – No mapa de uma rede social, é provável que cada "nó" (i.e., círculo no mapa) represente uma conta do Twitter ou um perfil do Facebook. No entanto, são as *relações* entre os nós (interações por meio de curtidas, "seguindo", *retweets* etc.) que servem de alicerce para a estruturação de uma rede de nós relevantes. Ou seja, o tipo de relação determina o esqueleto do mapa, a partir do qual são extraídas as conexões relevantes entre os nós. Na teoria dos grafos - ramo da ciência da computação dedicado a redes e mapas -, essas conexões também são chamadas de *arestas*.
3. **Poda dos Dados** – Na coleta de grandes volumes de dados, é bastante comum que a base de dados capturados seja superior à capacidade de mapeamento. Ferramentas como Affinio, NodeXL e Gephi, por exemplo, tendem a operar melhor processando numa faixa de poucos milhares de nós. Mapear em escalas maiores não costuma ser financeiramente vantajoso do ponto de vista computacional - por isso, é importante definir o tipo de rede mais relevante para cada caso. Na ciência da computação, o processo de remoção de dados descartáveis é comumente chamado de *poda* (*pruning*), ou,

11 Por exemplo, no grafo citado acima da modelagem do contágio de um vírus, as arestas podem ser direcionadas de acordo com a proliferação da infecção. Nesse caso, a aresta partiria do vetor em direção ao indivíduo contaminado e seria retratada por uma seta.

12 No exemplo de grafo acima retratando aeroportos, os valores das arestas podem refletir a distância em quilômetros entre aeroportos ou o tempo de viagem necessário entre um aeroporto e outro.

13 Para mais exemplos de redes de seguidores, veja a matéria da revista Wired (aqui) sobre uma rede de contas que circulam mensagens antivacina.

alternativamente, *redução de dimensionalidade*. Em algumas ferramentas, como as desenvolvidas pela Graphika, esses dados são removidos automaticamente, mas é possível realizar a triagem dos dados por conta própria com ferramentas como o Gephi. Podemos citar como exemplo de poda o mapeamento somente dos nós que utilizaram determinada *hashtag* relativa a uma eleição mais de uma vez ou a inserção somente dos nós conectados a cinco ou mais nós dentro da rede. [14]

4. **Elaboração do Mapa** – Uma vez determinadas as relações a serem mapeadas (arestas) e selecionados os nós mais relevantes, já é possível elaborar o mapa. Geralmente os dados selecionados são salvos em um formato aceito na ferramenta utilizada (por exemplo, CSV, .graphml ou *.gexf* para Gephi) e processados no software. A maior parte do trabalho pesado é automatizada. No YouTube, é possível encontrar diversos tutoriais disponíveis gratuitamente que são úteis para a elaboração de mapas de redes utilizando o Gephi[15] e outras ferramentas *open source*.
5. **Análise do Mapa** – Após a elaboração do mapa, o analista já pode personalizar as opções de visualização e iniciar a análise. Normalmente, métricas de *centralidade* são imprescindíveis para captar as dinâmicas de influência em uma rede. Sobre esse tópico, vale a pena consultar o livro *Analyzing Social Networks*[16] (Borgatti, Everett e Johnson 2019), que contém um capítulo inteiro dedicado aos diferentes tipos de centralidade.[17]

Exemplos de Rede

Como já exposto, uma mesma base de dados pode gerar diversos tipos de rede. O principal fator para definir o tipo de rede a ser mapeada é a *relação* que se quer visualizar. Mapas gerados a partir do Twitter costumam refletir redes direcionadas compostas por relações de seguidores e de *retweets*. Esses dois tipos de rede podem ser úteis para analisar dados e dinâmicas de influência.

Redes de Seguidores

Nesse tipo de rede, os nós representam contas do Twitter e as conexões entre os nós, as relações de "seguindo". Essas conexões costumam ser direcionadas (ligam dois nós em determinado sentido). Imagine que toda linha significa "*seguindo*". O grafo abaixo ilustra dois nós, A e B, sendo que "A *segue* B".

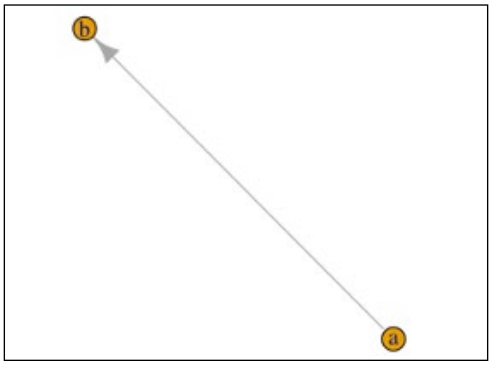


Ilustração de uma relação de "seguindo" unidirecional – no diagrama, A é seguidor de B, o que está evidenciado por uma única linha direcional (ou seta) de A até B.

Perceba que se trata de um grafo unidirecional - ou seja, A segue B, mas B não segue A. Se se tratasse de uma relação mútua, a seta seria bidirecional, como demonstrado na figura abaixo.

14 Esse tipo de poda é conhecido como *redução do k-core*.
15 O Gephi também disponibiliza um tutorial gratuito em PDF e outros materiais de apoio em seu site oficial: gephi.org.
16 "Analisando as Redes Sociais" em tradução livre.
17 Capítulo 10, "*Centrality*" ("Centralidade"). O livro é muito instrutivo para aprender o básico sobre redes e métodos para a análise de redes. Como de praxe, existem vários tutoriais *open source* excelentes disponíveis gratuitamente na internet.

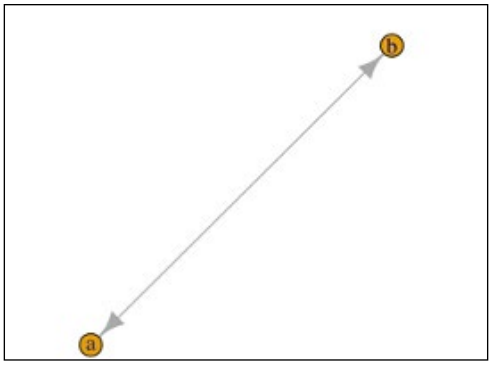


Ilustração de uma relação de "seguindo" mútua: A é seguidor de B, e B é seguidor de A.

Em redes geradas a partir de dados do Twitter referentes a eleições, provavelmente serão muito mais do que dois nós interligados. Os exemplos acima servem para ilustrar os componentes básicos de uma rede complexa.

Vantagens e Desvantagens de Redes de Seguidores

Particularmente no Twitter, relações de "seguindo" são relativamente duradouras e permanentes – é raro usuários deixaram de seguir outros usuários. Por isso, esse tipo de rede é considerado um retrato mais consistente das dinâmicas e dos fluxos de informação do que redes de *retweets*. Por outro lado, os usuários do Twitter tendem a ter mais de um interesse, tornando os seguidores de determinada conta potencialmente menos relevantes para o conteúdo analisado. Redes automatizadas costumam ser mais monotemáticas, focando, por exemplo, no apoio a um partido, candidato ou tema, mas, mesmo assim, há certa pluralidade de conteúdo. Esse é certamente um fator a ser considerado na análise de processos automáticos ou outros tipos de atividade coordenada em contas de redes sociais.

Num mapa hipotético do espectro político dos EUA, seria perfeitamente plausível, por exemplo, encontrar laços fortes entre uma rede de contas cujo assunto predominante é cultura e música pop e uma rede de contas ligadas preponderantemente à política.

É importante ponderar as vantagens e as desvantagens na hora de avaliar se a rede de seguidores interessa à pesquisa.

Redes de *Retweets*

Redes de *retweets* retratam outro tipo de relação no Twitter – nesse tipo de rede, as conexões entre os nós representam *quem retweetou para quem*. Desse modo, os mapas gerados são mais orientados pelo conteúdo do que aqueles gerados a partir das relações de "seguindo". Abaixo, um exemplo de arestas nesse tipo de grafo.

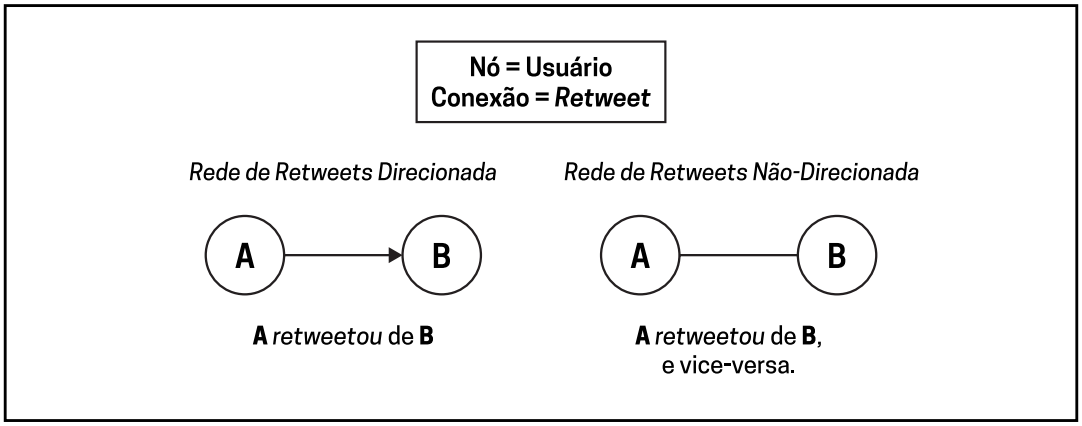
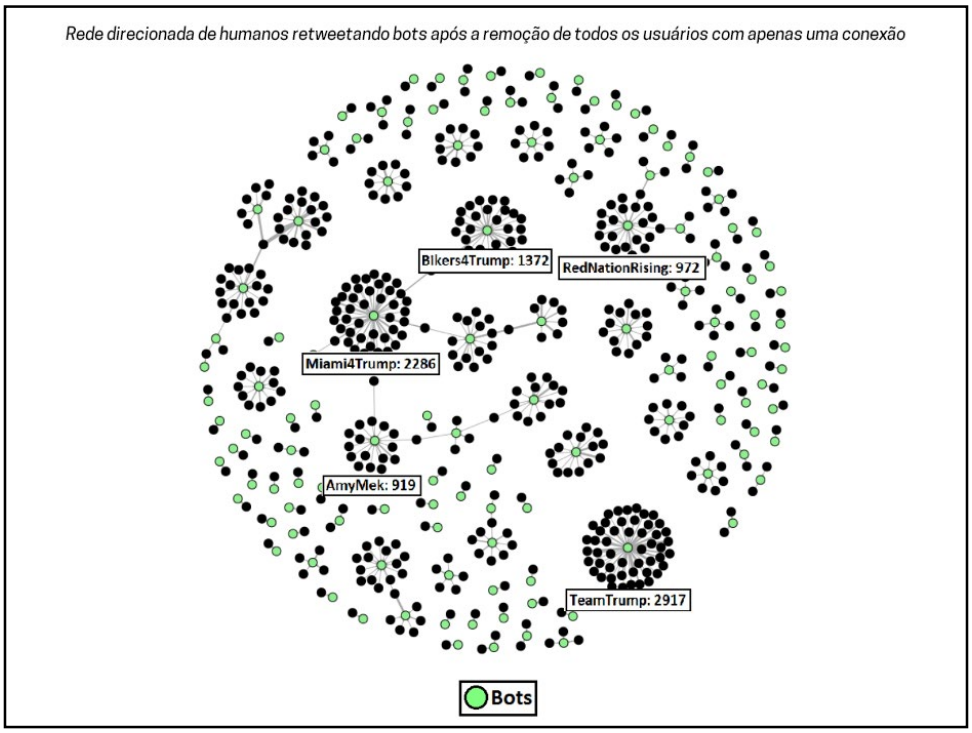


Diagrama ilustrando os nós e as arestas em uma rede de retweets. (Fonte: Samuel Woolley e Douglas Guilbeault [2017]. Computational Propaganda in the United States: Manufacturing Consensus Online [18]. Disponível aqui.)

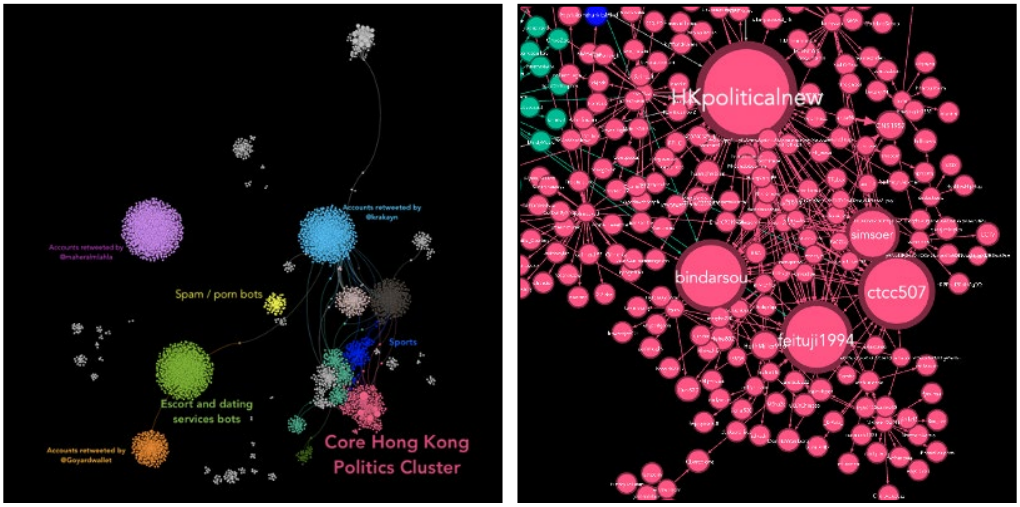
18 Propaganda Computacional nos EUA: Fabricando o Consenso na Internet" em tradução livre.

Vantagens e Desvantagens de Redes de *Retweets*

Redes de *retweets* são um pouco mais efêmeras do que redes de seguidores. Elas retratam uma fotografia do momento: quem *retweetou* para quem dentro de determinado intervalo de tempo. Por esse motivo, redes de *retweets* representam com certa precisão dinâmicas de influência dentro de intervalos de tempo curtos – como em casos de campanhas via *hashtag* ou as vésperas de uma eleição.



Rede de retweets *gerada a partir de dados coletados do Twitter durante as eleições presidenciais dos EUA de 2016. Os pontos verdes (nós) representam contas operadas por* bots *e os pontos pretos, contas pertencentes a humanos. A partir do mapeamento de* retweets *entre os usuários, é possível observar o número significativo de* retweets *com conteúdo gerado por* bots propagados *por humanos durante as eleições. (Fonte: Samuel Woolley e Douglas Guilbeault [2017].* Computational Propaganda in the United States: Manufacturing Consensus Online*. Disponível aqui.)*



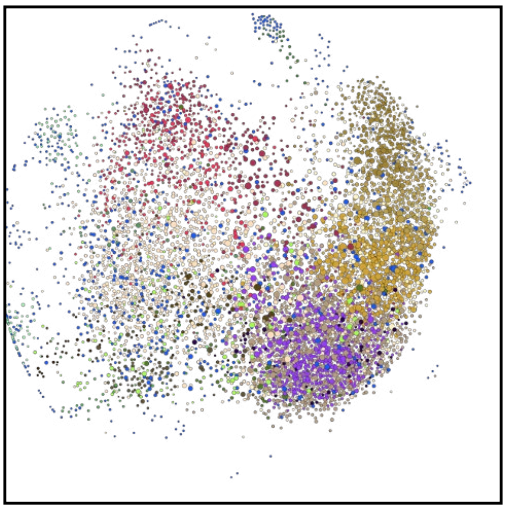
Imagens de uma rede de retweets *de contas do governo chinês disseminando desinformação para desprestigiar manifestações pró-democracia em Hong Kong entre junho e agosto de 2019. A rede foi desenvolvida com base no acervo de operações informacionais do Twitter[19]. À esquerda, uma imagem integral da rede de* retweets *e, à direita, uma perspectiva ampliada do principal cluster político tendo como alvo Hong Kong.* (Fonte: relatório elaborado pelo Laboratório de Inteligência Digital do Instituto para o Futuro [Digital Intelligence Lab - Institute for the Future, ou DigIntel], disponível aqui.)

19 Especificamente na disparada de *tweets* em agosto de 2019 atribuída ao governo chinês.

Redes de Menções

Mapas de menções também são comuns na análise de redes sociais. A concepção é parecida com os mapas de *retweets*, mas com arestas representando "menções", ou seja, episódios em que um usuário menciona outro.

Abaixo, é possível visualizar a rede de menções desenvolvida pela Graphika com base em dados da plataforma Gab compilados pelo Pushshift.io. O mapeamento foi realizado visando à análise de conversas e comunidades da plataforma, uma rede social bem similar ao Twitter em termos de funcionalidade e arquitetura.



O mapa de menções a usuários da rede social Gab desenvolvido pela Graphika. Os dados foram compilados a partir do banco de dados referente à plataforma disponibilizado gratuitamente pelo Pushshift.io, abrangendo um período que vai de agosto de 2016 ao final de outubro de 2018.

Além dos três tipos de rede mencionados, existem diversas outras possibilidades de mapeamento a partir de dados coletados do Twitter. Em outras plataformas, como Facebook e Gab, podem ser mapeadas relações de outra natureza: um exemplo seria o mapeamento de uma rede de curtidas entre páginas públicas.

Limitações da Coleta de Dados e do Mapeamento de Redes

Como todo artifício, a coleta de dados e o mapeamento de redes possuem certas limitações, principalmente no que tange à *escala* e à *cronologia* dos dados.

Como mencionado na seção sobre coleta de dados, todas as ferramentas de mapeamento - gratuitas ou pagas - disponíveis atualmente possuem limitações de escala, uma vez que, com o aumento do número de nós em uma rede, o número de possíveis conexões cresce *exponencialmente*[20], gerando uma quantidade de dados que mesmo computadores têm dificuldade de processar. E é raro encontrar ferramentas com capacidade para gerar mapas com mais de 15 mil nós.[21]

No entanto, seria um erro enxergar essa limitação exclusivamente como um problema - uma parte importante da ciência e da análise de dados envolve a seleção dos segmentos de dados mais propensos a gerar *insights* a partir de amplas bases de dados. Em outras palavras, uma análise de dados bem feita requer uma avaliação de quais dados mais merecem ser investigados. É por esse motivo que a ciência de dados é considerada tanto uma arte quanto uma ciência. A triagem dos dados, que é parte fundamental da pesquisa, da análise e da manipulação de dados, nem sempre é favorecida pela abundância de dados.

A segunda limitação comumente encontrada durante a coleta de dados e o mapeamento de redes refere-se a restrições de ordem temporal, especificamente em relação à captura de dados históricos. Por exemplo, a API de busca padrão do Twitter (*Twitter Search API*) só disponibiliza dados armazenados até uma semana antes da data de consulta. Para coletar dados anteriores a 7-9 dias, é necessário recorrer a outros meios, como adquirir ferramentas (pagas) que possuem essa função ou comprar dados diretamente de um provedor como o GNIP. Por mais úteis que sejam para a análise, dados históricos podem custar caro. Por isso, **a melhor solução é sempre coletar todos os dados relevantes em tempo real**. Se uma equipe de analistas almeja capturar dados em torno de uma eleição em tempo real, é sempre recomendável iniciar a coleta assim que os focos de interesse estiverem delineados.

20 Para quem se interessar pela matemática, uma rede de *n* nós possui *n*(n-1)/2* conexões possíveis.

21 Atualmente, o software de mapeamento da Graphika tem capacidade para mapear na maior escala possível, permitindo a visualização de até 5,5 milhões de nós.

Redes Fechadas e Criptografadas

Nos últimos anos, um dos desafios do monitoramento dos meios de comunicação é a popularidade e a proliferação de aplicativos de mensagens criptografadas, como WhatsApp, Telegram e Signal. Essas plataformas são cada vez mais utilizadas como fontes de informação sobre o ambiente político em períodos eleitorais e outros acontecimentos políticos relevantes. Em países como Brasil, Índia e México, por exemplo, houve um notório aumento de mensagens políticas transmitidas por meio do WhatsApp. Por mais que sejam indubitavelmente benéficas em termos de privacidade, segurança e direitos digitais, as redes de mensagens criptografadas trouxeram novos obstáculos para a compreensão da disseminação de informações políticas na internet.

Os melhores métodos praticados atualmente para o monitoramento de redes fechadas se apoiam na checagem manual de fatos - equipes de especialistas monitoram canais de indivíduos ou grupos relevantes no WhatsApp, checam a veracidade das postagens e compartilham os resultados encontrados publicamente. Existem diversas iniciativas bem-sucedidas de checagem de postagens, como o detector de WhatsApp do portal La Silla Vacía[22] na Colômbia e as realizações do coletivo Verificado[23] no México e do Centro para a Democracia e o Desenvolvimento (Center for Democracy and Development ou CDD) na Nigéria.[24]

Outra iniciativa digna de menção é o *bot* CoFacts, de Taiwan. Johnson Liang e uma equipe de desenvolvedores criaram, em parceria com o movimento g0v, um método de compartilhamento automatizado de checagem manual de fatos para ajudar cidadãos taiwaneses a verificar a veracidade das postagens. O *bot* CoFacts[25] pode ser adicionado no LINE, um aplicativo de mensagens criptografadas popular em Taiwan e no Japão, e o usuário que se deparar com uma postagem suspeita pode colar o *link* num *chat* com o *bot*. Se a postagem for inédita, uma equipe de humanos realiza a checagem dos fatos e envia uma mensagem com um resumo da veracidade da postagem para uma base de dados central. Depois a mensagem é reenviada pelo *bot* ao usuário original e a outros usuários interessados. O CoFacts disponibiliza publicamente dados anônimos coletados no Github e permite que usuários consultem a base de dados por meio de um site público.

A Meedan, uma empresa que apoia a checagem de fatos e outras pesquisas *online*, também lançou uma série de ferramentas similares no Check com o objetivo de ajudar usuários a automatizar e administrar coletivamente fluxos de trabalho para a checagem de fatos no WhatsApp e em outras plataformas.

Determinadas ferramentas, como o aplicativo Backup WhatsApp Chats, permitem que usuários exportem conversas do WhatsApp para arquivos CSV, mas o usuário deve pertencer a um canal para exportá-las. O aplicativo de mensagens criptografadas Telegram possui uma API que permite que usuários acessem canais públicos por código. Embora o Telegram propicie alguma dose de monitoramento público, os dados capturados no Twitter são mais valiosos.

Ferramentas e Pacotes Úteis para a Visualização de Redes

A tabela abaixo contém ferramentas e pacotes de código popularmente utilizados na visualização e na análise de redes.

Ferramentas para a Visualização e a Análise de Redes			
Ferramentas *Open Source*/Gratuitas	**Ferramentas Pagas**	**Pacotes Comumente Utilizados (Python)**	**Pacotes Comumente Utilizados (R)**
Gephi NodeXL	Graphika Affinio	networkx matplotlib igraph	igraph plotrix

22 https://www.niemanlab.org/2017/03/to-slow-the-spread-of-false-stories-on-whatsapp-this-colombian-news-site-is-enlisting-its-own-readers/
23 https://www.niemanlab.org/2018/06/whatsapp-is-a-black-box-for-fake-news-verificado-2018-is-making-real-progress-fixing-that/
24 https://www.cddwestafrica.org/whatsapp-nigeria-2019-press-release/
25 O nome do bot em chinês é 真的假的, ou "verdadeiro ou falso".

Identificando Influenciadores, Grupos e Contas

O objetivo da análise de dados é entender a distribuição de informações dentro de uma rede. Quais histórias estão despertando mais interesse? Quem são os usuários mais influentes? Quais são os portais de notícia mais citados nas conversas? Uma base de dados sólida, somada às ferramentas adequadas, permite que essas perguntas sejam respondidas ao nível dos detalhes, contribuindo para a apreensão da dinâmica de disseminação de informação no espaço virtual analisado.

Existem dois métodos para interpretar as dinâmicas de influência em redes sociais: com base no *conteúdo* e com base nos *atores*. A seguir, vamos explorar cada um desses métodos.

Identificando Dinâmicas de Influência com base no Conteúdo

Em métodos baseados em conteúdo, são utilizados principalmente *tweets*, *hashtags*, palavras-chave ou sites (na forma de URLs ou domínios[26]. Em alguns casos, os atores relevantes serão conhecidos - por exemplo, veículos ou políticos que estão constantemente disseminando desinformação. No entanto, é muito comum se deparar com fontes de desinformação, discurso de ódio e outros tipos de conteúdo analisado que não são de conhecimento público.

Na análise de conversas e outras manifestações políticas na internet durante períodos eleitorais, é altamente recomendável saber quais tipos de conteúdo estão despertando mais interesse - especialmente quando não são identificados atores específicos na base de dados. Nesse caso, um bom ponto de partida talvez seja selecionar quais URLs ou *tweets* estão ganhando mais adesão.

Tweets

Na análise de *tweets*, o poder de influência pode ser mais ou menos mensurado pelo número de *retweets* e/ou curtidas[27]. Seja utilizando ferramentas de coleta de dados de terceiros ou acessando as APIs do Twitter, analistas não deverão ter maiores empecilhos para capturar os dados independentemente da data de coleta. Uma vez selecionados, os *tweets* mais influentes podem servir de base para uma análise mais aprofundada. Eis algumas questões pertinentes a serem investigadas nesse tipo de análise:

- Quem postou o *tweet* originalmente? Quem *retweetou* a postagem? Qual é o tipo de perfil seguido por esses usuários? Se forem muitos, talvez seja válido mapear a rede de usuários.
- Quais *hashtags* são usadas no *tweet*? Se alguma *hashtag* chamar atenção ou for disparada somente por alguns poucos usuários, existe algo em comum entre esses usuários?
- Quais URLs estão presentes na postagem? Se for uma URL suspeita (criada recentemente ou propagadora de desinformação), talvez seja interessante investigar mais a fundo – por exemplo, verificando o histórico de registros de domínio no Whois[28] ou pesquisando, no Twitter, por outras menções pertinentes à mesma URL. Outra opção é usar a extensão do CrowdTangle para avaliar se a URL está ganhando adesão nas plataformas Facebook, Instagram ou Reddit ou em outros ambientes do Twitter.

As mesmas estratégias e os mesmos princípios se aplicam ao Facebook, ao Twitter, ao Gab e a outras plataformas de mídia social - a análise de interações em torno de uma postagem é uma maneira confiável de medir a influência de uma mensagem em determinada comunidade.

---

26 URLs são *links* completos que dão acesso a uma matéria ou a um site específicos. Domínios referem-se ao site de hospedagem do conteúdo - que corresponde ao texto anterior ao domínio de topo (ou TLD, da sigla em inglês para *top-level domain* – p.ex., "*.org*", "*.com*", "*.gov*" etc.) ou ao próprio TLD. Por exemplo, as URLs "exemplo-site-notícias.com/matéria1", "exemplo-site-notícias.com/matéria2" e "exemplo-site-notícias.com/matéria3" estão todas hospedadas no mesmo domínio: "exemplo-site-notícias.com".

27 É importante ter em mente que *tweets* tendem a receber mais curtidas do que *retweets*, assim como a maioria das postagens do Facebook recebem mais curtidas do que compartilhamentos. Qualquer anomalia nessas premissas pode ser interpretada como um sinal de atividade inautêntica, embora seja impossível afirmar com certeza.

28 O Whois disponibiliza diversos bancos de dados para a conferência de detalhes dos registros. A Corporação da Internet para Atribuição de Nomes e Números (*Internet Corporation for Assigned Names and Numbers* ou ICANN) mantém um banco de dados confiável, disponível em https://lookup.icann.org/.

Hashtags/Palavras-chave

Hashtags são naturalmente uma das principais entidades a serem investigadas ao se analisar o Twitter e outras redes sociais. O hábito de utilizar uma *hashtag* (#) para dar destaque ao tópico de um *tweet* é uma dádiva para pesquisadores - isso permite a captura de conversas relevantes sobre um tema de interesse com extrema facilidade. Existem diversas possibilidades para aprofundar a análise sobre uma *hashtag* ou um conjunto de *hashtags* de interesse, como pesquisar as *hashtags* que mais aparecem simultaneamente, desmembrar menções às *hashtags* por tempo ou pesquisar as URLs concomitantes.

URLs/Domínios

URLs e domínios postados no Twitter - na maioria das vezes, *links* para portais de notícia – são fontes extremamente úteis para avaliar quais conteúdos, publicações ou narrativas estão despertando mais interesse em determinada comunidade virtual.

Na análise de URLs ou domínios, um primeiro passo recorrente é extrair URLs específicas e contar o número de vezes que elas são mencionadas na base de dados. Apesar de simples e contundente, essa técnica está sujeita a diversas intempéries que, por mais sutis que sejam, podem ter repercussões. Para que os *insights* gerados na análise sejam mais precisos e proveitosos, vale a pena se atentar a algumas das questões abaixo.

- **Solucionando URLs encurtadas** – URLs postadas no Twitter são geralmente encurtadas devido ao limite de caracteres – utilizando uma ferramenta de ajuste, é possível reproduzir as URLs encurtadas na íntegra. Determinadas ferramentas (p.ex., URLex.org) disponibilizam uma API para que as URLs sejam expandidas automaticamente. Essa é a melhor maneira de garantir que dados relevantes não passem despercebidos por causa do encurtamento de URLs.
- **Padronizando URLs** – O mesmo domínio pode ser citado usando sequências (strings) de texto distintas[29]. Por exemplo, *links* para o *New York Times* podem ser escritos como "*www.nytimes.com*", "*nytimes.com*", "*NYTimes.com*", "*http://nytimes.com*", "*nyti.ms*", "*https://nytimes.com*", "*http://www.nytimes.com*", "*https://www.nytimes.com*" ou "*m.nytimes.com*" (existem muitas outras combinações possíveis). Para que a influência de uma URL ou de um domínio não seja subestimada devido à contagem de *strings* de texto distintas, é importante padronizar o formato antes de iniciar a contagem. Nem sempre será possível controlar as múltiplas formas de acesso a um mesmo conteúdo conectado por meio de URLs, mas um pouco de precaução com a padronização tem tudo para tornar a análise mais robusta. Durante a padronização, é importante se atentar a: (1) maiúsculas e minúsculas (*case sensitivity*[30]), (2) prefixos ("http://", "https://", "www.", "ww2." etc.) e (3) subdomínios, dentre outros fatores.

Uma vez identificadas as URLs mais populares em determinada série de dados, são muitas as possiblidades para aprofundar a análise. Se for um domínio de uma fonte de notícias recém-criada, é possível usar técnicas de inteligência de fontes abertas (*open-source intelligence* ou OSINT), como verificar as informações de registro do domínio para gerar *insights* a partir das conexões relativas a ele. Técnicas de inteligência de fontes abertas são úteis para ampliar o leque de informações sobre contas ou sites de interesse. Esse é um ramo em mutação constante, com ferramentas e técnicas aparecendo e desaparecendo cotidianamente. Existem muitas fontes que ensinam novas técnicas: uma das melhores é o portal Intel Techniques. O coletivo de pesquisadores Bellingcat, constantemente dedicado à documentação de operações de influência russas, se tornou perito na utilização de técnicas de OSINT para a reprodução de matérias jornalísticas pioneiras e disponibiliza publicamente, no Google Docs[31], um inventário pormenorizado de ferramentas de investigação e de inteligência de fontes abertas. Lawrence Alexander, um cientista de dados instalado no Reino Unido, teve a engenhosidade de recorrer aos códigos do Google Analytics para mapear uma rede de sites pró-Kremlin em 2015.

Após a triagem dos sites e dos artigos mais influentes, também é recomendável avaliar os tipos de conteúdo para examinar as narrativas presentes. Técnicas de PLN (processamento de linguagem natural) - como o emprego da frequência de n-gramas para analisar as expressões mais comuns utilizadas nos artigos, do cálculo tf-idf para comparar temas afins em artigos distintos ou de métodos de análise qualitativa - podem se mostrar reveladoras.

29 No contexto da computação, dados textuais também são chamados de "*strings*", uma abreviação de "*strings of characters*", ou "sequência de caracteres". É assim que cientistas da computação, às vezes, se referem ao texto encontrado nos/nas *tweets*/postagens em bases de dados de redes sociais.

30 *Case sensitivity* é um termo em inglês que indica se os dados textuais estão em caixa alta ou caixa baixa. Esse tipo de problema é facilmente contornável formatando todas as URLs da série em caixa baixa antes de iniciar a contagem do número de ocorrências de cada URL. Mas é importante ter em mente que, embora a maioria das URLs completas não sejam *case sensitive*, muitas URLs encurtadas são. Por isso, é recomendável que as URLs sejam solucionadas antes de serem formatadas em caixa baixa ou padronizadas.

31 https://docs.google.com/document/u/1/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit

Análise Baseada em Redes

Outra maneira de analisar as dinâmicas de influência é se baseando em uma rede. Essa abordagem consiste no mapeamento de uma rede relevante a partir dos dados coletados, como debatido na seção *Análise de Dados e Redes* - por exemplo, redes de menções, de seguidores, de *retweets* ou outras métricas semelhantes.

Clusterização/Grupos

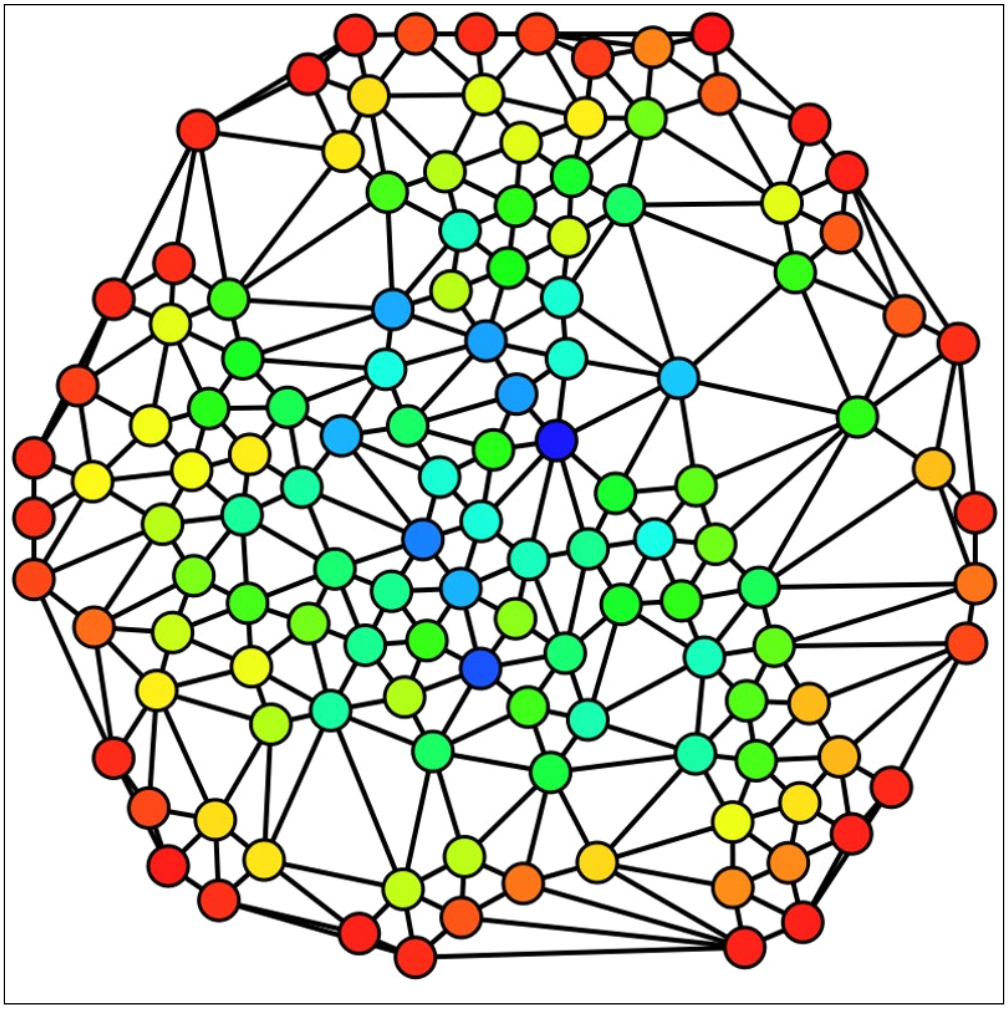
A detecção de comunidades (geralmente chamadas de *clusters* [aglomerados] na ARS) é a base da maioria das análises comparativas relevantes entre comunidades. Embora diversos algoritmos para clusterização estejam embasados em teorias metodológicas complexas, o grosso do trabalho é realizado automaticamente por qualquer um dos softwares utilizados. O Gephi oferece várias opções de visualização e clusterização de comunidades (mais detalhes neste tutorial). A Graphika também possui recursos para gerar *clusters* automaticamente. Em suma, uma vez identificadas as diferentes comunidades de uma rede pelo software de visualização e análise, já é possível passar para a análise qualitativa para avaliar o que os membros de determinado *cluster* têm em comum.

Muitas vezes, comunidades ou *clusters* de contas apresentam semelhanças tangíveis, como a disseminação de fontes de notícias comuns ou a filiação a partidos similares. São nessas circunstâncias que a compreensão do contexto político mais abrangente se torna importante. A melhor forma de apontar as características em comum de membros de determinada comunidade é conjugando análises quantitativas e qualitativas.

Centralidade

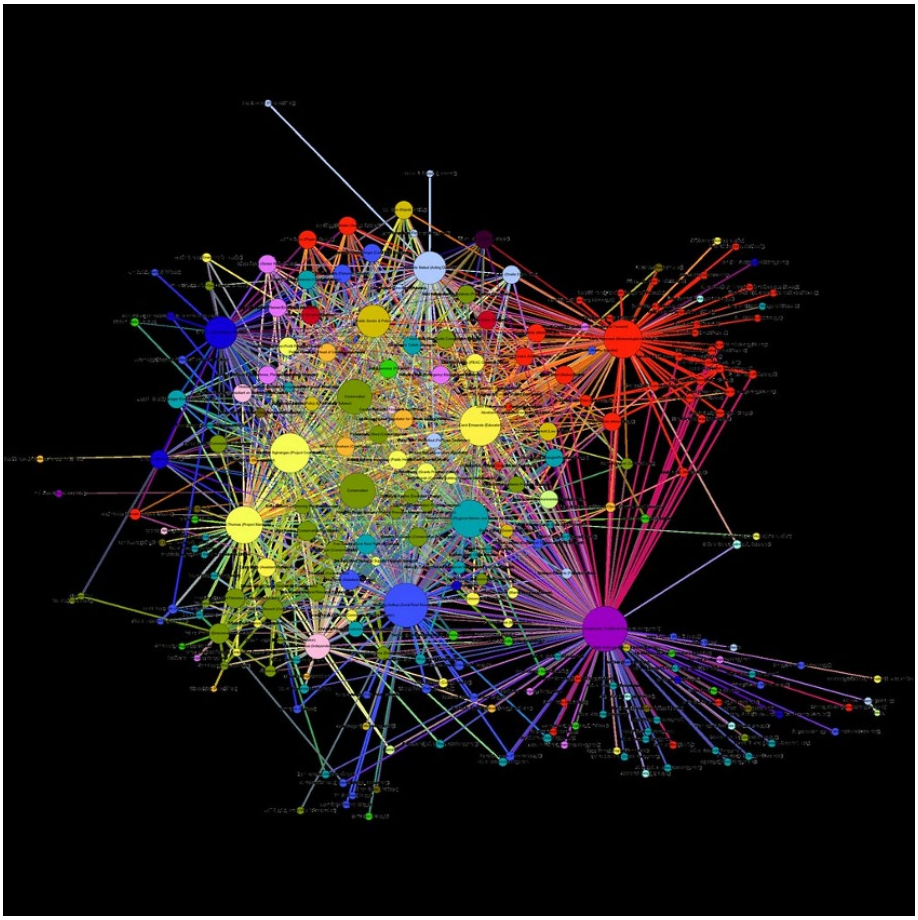
Na teoria das redes, especificamente quando aplicada na ARS, a principal métrica para se analisar a influência de um ator ou de um grupo de atores é a *centralidade*, que mede a intensidade de conexões (poder de influência) de determinado nó dentro de uma rede. Existem diversos métodos para medir a centralidade.

- **Centralidade de grau** – Em grafos não-direcionados, a centralidade de grau de determinado nó é medida pelo número de conexões diretas com outros nós em volta. Em grafos direcionados, compostos por arestas com sentido definido, existem dois tipos de centralidade de grau: centralidade de grau de entrada (*in-degree*), medida pela quantidade de conexões recebidas por um nó, e centralidade de grau de saída (*out-degree*), medida pela quantidade de conexões procedentes de um nó. Em análises de dinâmicas de influência, a centralidade de grau de entrada será provavelmente mais relevante - um nó com muitas conexões recebidas tende a ser muito influente. Esse raciocínio é relativamente intuitivo: uma conta com 15 mil seguidores (15 mil conexões recebidas) tem mais capacidade de influência direta do que uma conta com 100 seguidores. A importância do tipo de centralidade de grau em grafos direcionados varia de acordo com a rede analisada.
- **Centralidade de intermediação** – Centralidade de intermediação pode ser entendida como a capacidade de propagação de mensagens no tempo por parte de um nó. Ou seja, quanto maior a capacidade de viralização e disseminação de mensagens no tempo, maior é o escore recebido pelo nó. Esse valor é estimado contando o número de vezes que um determinado nó percorre o trajeto mais curto até outros nós.



A tonalidade (do vermelho=0 ao azul=máx.) indica a centralidade de intermediação de cada nó. (Claudio Rocchini) Creative Commons BY 2.5 https://en.wikipedia.org/wiki/Social_network_analysis#/media/File:Graph_betweenness.svg

- **Centralidade de autovetor** – A centralidade de autovetor é muito útil para avaliar as dinâmicas de influência em determinada rede ou sub-rede. A ideia por trás da centralidade de autovetor é basicamente "Quem influencia os influenciadores?". Para medir a influência nesse tipo de centralidade, o número total de laços estabelecidos por nó é menos importante do que a conectividade dos laços. É como se a rede de influência estivesse sendo investigada "por gotejamento" - com que probabilidade informações são disseminadas de um nó matricial para outros nós influentes? O buscador do Google aplica esse conceito: uma página (ou nó) é ranqueada de acordo com o número de páginas que fazem referência a ela. Nós com elevada centralidade de autovetor talvez sejam particularmente ativos na disseminação de bens (como dinheiro, informação, germes etc.) dentro de uma rede.



Projeto de Análise de Redes Sociais da Pacific RISA, com um mapa centrado em Palau; todos os membros são de Palau ou possuem ligação com o arquipélago. Os nós estão dimensionados de acordo com a centralidade de autovetor, e cada cor representa uma profissão. Creative Commons BY 2.5 https://www.flickr.com/photos/pacificrisa/11344578486

- **Pontes** – Embora não possam ser caracterizadas como um tipo de centralidade, *pontes* são fenômenos de estruturas de rede úteis para se ter em mente. Um nó ou um punhado de nós serve como *ponte* quando conecta dois *clusters* importantes. Pontes são imprescindíveis para que *clusters* diferentes (como filiados de dois partidos políticos distintos ou adeptos políticos de dois países distintos) transmitam informações entre si ou se comuniquem. Nesse sentido, pontes são essenciais para a viralização de conteúdos em redes *online*.
- **Folhas** – *Folhas* são nós com uma única aresta conectada à rede. Normalmente, é pertinente eliminar essas contas da rede, especialmente em redes relativamente grandes, já que é bem improvável que essas contas exerçam algum tipo de influência.

Existem diversos tutoriais e recursos disponíveis sobre os diferentes tipos de centralidade - vale a pena consultar o livro *Analyzing Social Networks* (Borgatti et al., 2013), que, no capítulo 10, explora os diferentes tipos de centralidade e o modo como são mensurados.

Ferramentas *open source* como o Gephi se encarregam da matemática complexa que calcula, em segundos[32], os diferentes tipos de centralidade. Em última instância, o tipo de centralidade fica a critério do analista e de sua equipe. Embora o ideal seja consultar um cientista de dados ou um teórico do ramo para determinar qual tipo de centralidade mais se aplica a cada caso, não é necessário se ater muito aos detalhes metodológicos - praticamente todos os tipos de centralidade partem do pressuposto de que os nós mais influentes são, de certa forma, aqueles com o maior número de laços dentro de uma rede ou sub-rede.

Uma vez definido o tipo de centralidade, é possível ainda personalizar a configuração visual da rede de acordo com o padrão adotado. No Gephi, por exemplo, o tamanho do nó ou a tonalidade de cor podem ser utilizados para salientar o tipo de centralidade.

32 Ou em minutos, dependendo do tamanho da rede analisada.

Identificando Fontes de Notícias

Particularmente para a análise de eleições e informações, a quantidade de fontes de notícias citadas nos dados é de suma importância. Nesse tipo de pesquisa, é especialmente recomendável trabalhar com pessoas que dominam o contexto social e político do país ou da região analisada, já que a tendência é que reconheçam as fontes de notícias mais frequentemente citadas. É importante ter uma noção bem clara do cenário midiático subjacente do país, como já examinado em outra seção, o que inclui conhecer a estrutura do mercado comunicacional e o poder de influência dos veículos de imprensa televisiva, radiofônica, impressa e *online*.

Existem vários métodos eficientes para a identificação de novas fontes de notícias em determinada região ou base de dados. Uma opção é realizar buscas regulares no Google por notícias e informações políticas da região (em línguas variadas se a região for plurilíngue). Fontes de notícias que almejam ampliar a influência costumam investir em estratégias de otimização para mecanismos de busca (*search engine optimization* ou SEO) para que tenham os sites evidenciados nas primeiras posições da busca do Google, e, muitas vezes, são portais recém-criados desconhecidos da maioria do público. Outra opção bastante recomendável é consultar a base de dados por menções a domínios ou URLs, o que pode ser realizado utilizando o CrowdTangle para monitorar as principais URLs de um conjunto de sites políticos ou convocando um especialista sobre a região para ajudar a extrair e pesquisar URLs/domínios[33] eminentes que não tenham sido identificados. O CrowdTangle disponibiliza gratuitamente um *plugin* para o Chrome e outros navegadores que permite a visualização de compartilhamentos de artigos específicos, embora o acesso ao *dashboard* e a outros recursos mais avançados só seja possível mediante uma licença institucional, geralmente obtida através do Facebook, atual controlador do CrowdTangle.

O importante a ser assimilado na análise é que, muitas vezes, a desinformação é propagada por sites (domínios) de curta duração criados especificamente para temas políticos e eleitorais. Um exemplo é o *streetnews[.]one*, um domínio criado e difundido na plataforma Gab às vésperas das eleições de meio de mandato dos EUA em 2018, que foi utilizado para a disseminação de conteúdo islamofóbico e sensacionalista e, em pouco tempo, desapareceu. Outro exemplo é a rede de desinformação iraniana Endless Mayfly, analisada em pesquisa do Citizen Lab da Universidade de Toronto (conduzida em parceria com especialistas da área). A equipe do laboratório se valeu do caso para cunhar o termo "*desinformação efêmera*", relativo a domínios com vida útil limitada que têm como objetivo propagar desinformação sobre temas estratégicos, eleições e campanhas.

Nessa etapa, pode ser extremamente profícuo consultar compilações de domínios destinados à desinformação ou de sites de *fake news*, tal como a lista desenvolvida por pesquisadores de Stanford, que reúne mais de 600 domínios conhecidos por terem produzido conteúdo falso no final de 2018, a maior parte direcionado aos EUA (Allcott et al, 2018)[34]. Ao consultar esse tipo de compilação, é importante ter em mente que: (1) a desinformação e a esfera virtual são dinâmicas - novos domínios destinados à desinformação capturados após a confecção da lista ficarão ausentes da análise; e (2) toda compilação deve passar por um escrutínio metodológico rigoroso antes de ser utilizada – consultas a listas aleatórias encontradas na internet podem comprometer a integridade da pesquisa.

Analisando Contas e Conteúdo

Quando os dados já estiverem coletados e/ou a rede com as contas de interesse relevantes estiver mapeada, o analista e sua equipe já podem dar início à análise das contas e do conteúdo contidos na série de dados. É provável que essa seja a tarefa que mais demandará tempo, especialmente se os objetos de investigação ainda não estiverem claros.

A melhor forma de analisar o conteúdo é alternar entre métodos quantitativos e qualitativos, repetindo o processo várias vezes até encontrar contas ou conteúdos de interesse específicos. Nesta seção, vamos dar algumas dicas e apresentar algumas ferramentas que podem ser úteis para esse tipo de análise.

33 De preferência, acompanhados da contagem de menções, uma aproximação da popularidade dos sites. Outros métodos, como extrair URLs das postagens mais *retweetadas* ou curtidas, também costumam ser utilizados para estimar a influência de determinado domínio numa base de dados.
34 O artigo pode ser acessado aqui.

Tipos de Conteúdo

Antes de se aprofundar nos dados, é bom ter uma noção dos tipos de conteúdo a serem investigados.

- **Desinformação/Má informação** – Um dos tipos de conteúdo mais nocivos a serem observados na base de dados são postagens políticas falsas e falaciosas. Existem inúmeras designações para conteúdo falso, como "propaganda computacional" ou "*fake news*", mas o fenômeno é mais conhecido como "desinformação" ou "má informação" (*misinformation*). Em tese, a única diferença entre os dois termos reside na intencionalidade da falsificação do conteúdo[35]. Neste guia, nos basearemos nas diferenças terminológicas apontadas no léxico de mentiras da *Data & Society* (*Lexicon of Lies* [Jack 2017]), que abarca um conjunto de vocábulos úteis para o debate sobre conteúdo falso na internet.
  - **Desinformação** – Conteúdo falso disseminado com a intenção deliberada de ludibriar. Atores estatais com interesse político ou atores com interesse financeiro são as fontes mais prováveis de propagação consciente de desinformação, como aqui compreendida.
  - **Má informação (*misinformation*)** – Informação falsa distribuída e propagada involuntariamente. Se uma conta compartilha uma notícia sem a intenção de enganar usuários, ela está disseminando informações de má qualidade (má informação).
  - **Informação maliciosa (*malinformation*)** – Alguns autores também vêm chamando a atenção para o fenômeno da "informação maliciosa" - a disseminação de informações verdadeiras ou predominantemente verdadeiras com propósitos lesivos. Claire Wardle e Hossein Derakhshan definem o conceito como "*informações baseadas na realidade, utilizadas para prejudicar uma pessoa, uma organização ou um país*" (Wardle e Derakhshan 2017).
- **Discurso de Ódio** – Discursos de ódio são enunciados destinados a demonizar indivíduos de determinada raça, etnia, gênero, orientação sexual ou religião. Muitas vezes, esse tipo de discurso tende a incitar episódios de assédio, difamação ou violência contra grupos sociais específicos.

Análise Linguística

Uma forma de realizar um exame rigoroso do conteúdo é por meio de uma análise linguística. Esse tipo de análise permite que sejam averiguados os principais idiomas utilizados nas mensagens, as principais pautas debatidas, as narrativas alimentadas e aprofundadas, palavras-chave e jargões recém-criados, bem como a presença de discursos de ódio e outros conteúdos nocivos nas conversas.

Palavras-chave e Léxicos

É provável que nem toda postagem e nem todo *tweet* coletados sejam relevantes para o objetivo da análise. Nesse caso, é recomendável realizar uma compilação de palavras-chave pertinentes ao tipo de informação pesquisado. A melhor forma de garantir a qualidade de uma compilação de palavras-chave é trabalhar com um especialista no objeto em foco, ou seja, alguém que domina a língua e a política da região de interesse. Essas compilações costumam ser chamadas de "léxicos" se forem tematizadas. Particularmente na análise de conteúdo político, muitas vezes são utilizados léxicos envolvendo discursos de ódio em línguas variadas relativos a contextos políticos distintos. Consultar um especialista, nem que seja por uma hora, pode ser extremamente frutífero para garantir o rigor e a qualidade de uma compilação de palavras-chave. Outra opção é recorrer a artigos acadêmicos consolidados e aproveitar listas já existentes, desde que sejam qualificadas e relevantes para o contexto.

Exemplos de Léxicos

Na internet, é possível encontrar exemplos de léxicos que podem servir para análises linguísticas e para a extração de postagens relevantes. O grupo de trabalho sobre Gênero, Mulheres e Democracia do NDI compilou um léxico de discursos de ódio nos idiomas indonésio, queniano e sérvio (Zeiter et al., 2019). A PeaceTech Lab, uma organização sem fins lucrativos dedicada à promoção da paz em países em desenvolvimento por meio do uso da tecnologia, também disponibiliza publicamente em seu site uma série de léxicos de discurso de ódio, todos plurilíngue, o que pode ser extremamente útil para o monitoramento de conversas em localizações distintas ou em regiões com alta diversidade linguística.

No site Hatebase.org, também é possível encontrar compilações de palavras-chave envolvendo discursos de ódio em diversos idiomas. O site serviu de base para uma pesquisa sobre propaganda computacional direcionada a americanos muçulmanos nas eleições de meio de mandato dos EUA em 2018 (2019), realizada pelos acadêmicos Roya Pakzad e Nilhoufar Salehi. Uma

35 Apesar da diferenciação, muitas vezes, é impossível saber a intenção por trás de conteúdos falsos disseminados na internet. Por isso, os dois termos costumam ser usados como sinônimos.

compilação similar foi utilizada para uma análise quantitativa da islamofobia na plataforma Gab às vésperas da mesma eleição (Woolley, Pakzad & Monaco, 2019).

Análise Linguística Qualitativa

Uma vez reunidas as postagens, já é possível se aprofundar na análise linguística. Na análise qualitativa, são examinados os conteúdos e os temas de postagens. Esse tipo de análise é mais efetivo quando realizado por humanos e conduzido por um especialista - ou uma equipe de especialistas - familiarizado com o contexto político e linguístico da região analisada.

Independentemente se a abordagem for qualitativa, quantitativa ou uma combinação entre as duas, o mais importante é que os métodos selecionados sejam consistentes e sistemáticos. Aplicar o mesmo conjunto de métodos para analisar todas as postagens ou todos os segmentos de dados é a melhor forma de se prevenir contra o enviesamento dos resultados.

Análise de Narrativas

Embora seja um método intensivo de análise do conteúdo linguístico, análises de narrativas podem ser muito interessantes. Analisar como a mídia trata determinado tema, especialmente em séries temporais, pode lançar luz sobre o enquadramento e o grau de influência dos meios de comunicação na opinião pública.

Codificação Qualitativa

Outro método qualitativo útil para decifrar o conteúdo das mensagens contidas em determinada série de dados é conhecido como *codificação* qualitativa, que consiste no trabalho realizado por profissionais especializados de agrupamento das postagens em categorias (ou "códigos") predefinidas. Cumprida essa etapa, já é possível realizar a análise quantitativa.

Vamos imaginar que a análise seja sobre uma eleição presidencial disputada por dois candidatos - candidatos A e B – no país fictício de Qumar[36]. Podemos vislumbrar cinco possíveis categorias para mensagens coletadas em torno da eleição:

1. Favoráveis ao candidato A
2. Favoráveis ao candidato B
3. Contrárias ao candidato A
4. Contrárias ao candidato B
5. Neutras

Depois que a equipe de especialistas tiver codificado todas as postagens da série de dados, eis algumas possibilidades de análise quantitativa:

- **Distribuição de postagens em cada categoria** – Uma possibilidade é analisar a quantidade de postagens em cada categoria para avaliar o apoio/a oposição aos candidatos A e B.
- **Utilização de palavras-chave por categoria** – Outra opção é pesquisar por palavras-chave relevantes nas postagens de cada categoria para examinar o vocabulário dos apoiadores e dos opositores de ambos os candidatos.
- **Conteúdos gerados por *bots* em cada categoria** – Também seria pertinente examinar conteúdos gerados por *bots* em cada categoria para avaliar a evolução do apoio e da oposição de assistentes automatizados a cada candidato.

Esses são apenas alguns exemplos de análises propiciadas por um trabalho de codificação qualitativa bem feito.

Análise Linguística Quantitativa

A análise linguística quantitativa, também conhecida como processamento de linguagem natural (PLN) ou linguística computacional, se baseia na ideia de que determinados *insights* sobre tipos e frequências de trocas de mensagens podem ser gerados a partir de uma concepção estatística da linguagem. Em termos mais palpáveis, agregando palavras ou conjuntos de palavras presentes em postagens relevantes, é possível avaliar as pautas das conversas. Nesta subseção, vamos apresentar noções básicas do método de extração de contagem de palavras em séries de dados, utilizado para investigar temas recorrentes na internet.

36 Qumar é um país fictício que aparece na série americana de drama político *The West Wing*.

Por mais que as técnicas descritas nesta seção possam ser implementadas utilizando qualquer linguagem de programação, existem diversos pacotes em Python e R que simplificam o processo, como o NLTK [37] para Python e o tm [38] para R. Esses pacotes estão amplamente documentados em livros e em guias e tutoriais disponíveis na internet, que ensinam o básico em poucas horas. É altamente recomendável reservar um tempo para se familiarizar com um desses pacotes, especialmente para aqueles que já têm uma noção de Python e R. Um pouco de dedicação extra no início pode reduzir consideravelmente o tempo empenhado na análise mais à frente!

N-gramas

N-gramas são os pilares de quase toda análise linguística quantitativa de conteúdos postados em redes sociais. N-gramas são sequências de *n* palavras. Existem três tipos de n-gramas mais frequentes na análise linguística quantitativa:

- **Unigrama** – Uma única palavra também é considerada uma "sequência" de uma palavra. Esse tipo de n-grama é conhecido como *unigrama*.
- **Bigramas** – Duas palavras *contíguas* em uma frase formam um bigrama. Ou seja, um bigrama é toda sequência de duas palavras dentro de um texto.
- **Trigramas** – Já deve estar claro que um trigrama é toda trinca de palavras presente em uma frase. Cada sequência de três palavras numa frase ou num texto forma um trigrama independente.

Esses são os três tipos de n-gramas mais utilizados. Em larga medida, isso se deve ao elevado "custo computacional" relativo ao processamento de sequências maiores - é provável que o desempenho do computador fique prejudicado, tornando-se pouco vantajoso do ponto de vista financeiro. Para sequências com mais de três palavras, a convenção é simplesmente digitar o número de palavras seguido de "-gramas". Por exemplo, uma sequência de quatro palavras seria escrita como "4-gramas", de cinco palavras, como "5-gramas" etc.

A principal vantagem da utilização de n-gramas é que, além de obter a contagem de palavras, é possível ter uma noção do *contexto* correspondente à palavra. Se, numa busca, aparecer a palavra "rei" 16 vezes, é sinal de que se trata de um tópico frequente. Mas não esclarece muito mais do que isso. Se a análise for ampliada para 4-gramas e aparecerem 15 ocorrências de "abaixo o rei" e uma ocorrência de "vida longa ao rei", é bem provável que a maioria das postagens da série de dados relativas a "rei" não seja de mensagens favoráveis.

Uma vez dominada pela equipe de analistas, a técnica de extração e contagem da frequência de n-gramas pode ser aplicada para diferentes segmentos da série de dados. Por exemplo, comparar n-gramas entre contas e páginas que apoiam diferentes candidatos/partidos políticos pode ser revelador; comparar a frequência de n-gramas de diferentes veículos de imprensa que produzem matérias relevantes sobre uma mesma eleição talvez ajude a esclarecer o principal foco de cada veículo; comparar a frequência de n-gramas entre históricos de postagem de duas contas ou páginas distintas pode lançar luz sobre os principais tópicos das mensagens. Esses são somente alguns exemplos de alternativas para o aprimoramento da pesquisa.

Outras Técnicas de Análise Linguística Quantitativa

O cômputo da frequência de n-gramas é uma técnica que pode ser empregada como uma introdução a outras técnicas de PLN capazes de contribuir para uma análise mais aprofundada dos dados. Após a extração da frequência de palavras ou n-gramas, uma possibilidade é aplicar uma técnica estatística conhecida como tf-idf [39] para comparar temas de mensagens entre documentos distintos, que podem ser desde coleções de matérias de veículos de notícia diferentes às vésperas de uma eleição a históricos de postagem de contas diferentes. A técnica tf-idf é uma forma simples de apontar os temas que distinguem dois documentos e pode servir para analisar quais contas promovem mais assiduamente determinado partido ou quais fatores singularizam mensagens associadas a uma comunidade específica.

Um guia básico sobre o uso da técnica tf-idf para análises linguísticas[40] e clusterização de conteúdo pode ser encontrado no livro *Mining the Social Web*[41] (Russell e Klassen 2018). Essa é uma fonte extremamente válida – o livro contém exemplos de códigos em Python e é particularmente fácil de ser digerido.

37 *Natural Language Toolkit*, um kit de ferramentas para processamento de linguagem natural.
38 Abreviação de "*text mining*", ou "mineração de texto".
39 *Term frequency - inverse document frequency*, ou "frequência de termos – frequência inversa dos documentos" em tradução livre.
40 O texto também oferece uma introdução a algumas técnicas relevantes para o aprimoramento da análise, como a remoção de *stopwords* (palavras de pouco valor informacional) e *stemming* (remoção de sufixos e prefixos).
41 "Minerando a *Web* Social" em tradução livre.

Detecção Automática de Discursos de Ódio

Na análise de discursos de ódio contidos em bases de dados, a primeira tarefa provavelmente consistirá em realizar uma compilação de termos sensíveis ligados a manifestações de ódio que sejam relevantes para a região analisada. Os termos devem ser examinados minuciosamente com a ajuda de um especialista no objeto em foco em todos os idiomas majoritariamente utilizados na região, conforme apontado na metodologia descrita no relatório *Tweets That Chill* (Zeiter et al., 2019), elaborado pelo NDI.

Um método heurístico para a detecção automática de discursos de ódio sem a necessidade de compilação de palavras-chave é por meio da API Perspective, uma ferramenta *open source* lançada em 2017 pela incubadora Jigsaw, pertencente ao Google. Atualmente, a API só presta assistência a comentários em língua inglesa[42]. A ferramenta gera um escore de toxicidade para cada sequência de caracteres introduzida no sistema, e o grau de toxicidade de um enunciado é determinado com base nos modelos de *machine learning* da API. Um exemplo de aplicação da interface pode ser encontrado na base de dados desenvolvida pelo site Pushshift.io referente à plataforma Gab. Além de armazenar as postagens da plataforma, o site testou cada postagem na API e registrou o escore de toxicidade correspondente.

A API Perspective é, atualmente, uma das poucas ferramentas publicamente acessíveis que atribui escores de toxicidade a elementos linguísticos. É extremamente trabalhoso e extenuante captar as nuances do contexto e da intenção na linguagem humana, o que explica a rudimentariedade das análises de sentimentos e das ferramentas de detecção de discursos de ódio. Além de toda a dificuldade inerente à questão, a especificidade de cada idioma e de cada contexto social associados à propagação de discursos de ódio representa um obstáculo a mais ao desenvolvimento de ferramentas de detecção automática criteriosas e confiáveis. Por isso, convocar especialistas no objeto em foco para compilar palavras-chave e léxicos segue sendo o melhor método para a análise de discursos de ódio em bases de dados de redes sociais.

Bots

A influência de *bots* em redes sociais tem sido um tema bastante estudado nos últimos anos. O Projeto de Propaganda Computacional (*Computational Propaganda Project* ou ComProp) da Universidade de Washington e do Instituto de Estudos da Internet da Universidade de Oxford (*Oxford Internet Institute* ou OII) realizou trabalhos pioneiros explorando a influência de *bots* na disseminação e na promoção de propaganda computacional em países mundo afora.

Simplificadamente, em plataformas de mídia social, *bots* são programas de computador que controlam perfis, geralmente simulando pessoas de verdade e interagindo virtualmente com outros humanos. A maioria dos *bots* que trafegam em redes sociais controlam contas por meio das APIs[43]. Os *bots* mais simples costumam dar sinais indicando que são automatizados - por exemplo, postam *tweets* no mesmo minuto toda hora ou não possuem fotos de perfil. Esses fragmentos de dados são geralmente usados em algoritmos de *machine learning* para ferramentas que distinguem *bots* de humanos conectados à internet.

Ferramentas para a Detecção de *Bots*

Embora seja quase sempre difícil determinar se uma conta é controlada ou não por um *bot*, pesquisadores interessados têm boas opções à disposição para a detecção de *bots* na internet. Atualmente, uma das melhores ferramentas de detecção é o Botometer, que utiliza *machine learning* para estimar a probabilidade de uma conta ser controlada por um bot. A ferramenta tem um histórico de pesquisa e desenvolvimento na Universidade de Indiana e pode ser baixada gratuitamente. Existem inúmeros outros classificadores disponíveis (veja a tabela abaixo).

42 A língua inglesa foi desproporcionalmente beneficiada pela atenção de linguistas ao longo dos séculos 20 e 21, incluindo de uma perspectiva computacional. Idiomas que não são beneficiados por pesquisas e pelo interesse despertado são caracterizados por possuírem uma baixa quantidade de *corpus* linguísticos disponíveis (no jargão da linguística e do PLN em língua inglesa, são denominados *low-resource languages*). A produção acadêmica relativa a esses idiomas deve ser louvada. Se o trabalho de monitoramento midiático contemplar pesquisas sobre discurso de ódio e linguística, talvez seja válido entrar em contato com linguistas profissionais ou acadêmicos para avaliar se essas pesquisas podem contribuir para ampliar o conhecimento no campo.

43 Na seção sobre coleta de dados, abordamos a distinção entre a extração de dados via APIs e *web scraping* - essa distinção também é útil para compreender como determinados *bots* operam em redes sociais e na internet sem a intermediação de APIs. *Bots* podem ser programados para interagir com sites rotineiros - na verdade, essa é uma tarefa um tanto banal para programadores. Por exemplo, *bots* podem percorrer diversos sites analisando o conteúdo das páginas - esses tipos de *bot* são geralmente chamados de *crawlers* ("rastejadores") e *spiders* ("aranhas"). É assim que o Google extrai dados das páginas para inseri-las no mecanismo de busca. Assim como nem todo *bot* está restrito às redes sociais, nem todo *bot* é nocivo. Aliás, alguns *bots* são necessários para o funcionamento cotidiano da internet.

Ferramentas de Detecção de *Bots*

Ferramenta	Pode ser implementada por código para a classificação de lotes de contas?	Plataforma[44]	Extensões/sites
Botometer	Sim (Python)	Twitter	Contas individuais podem ser verificadas no site
Tweetbotornot	Sim (R)	Twitter	Disponível somente a execução do código
Botcheck.me	Não	Twitter	Extensão do Chrome
Botsentinel	Não	Twitter	Aplicativo para Android e extensão para Chrome/Firefox
Pegabot	Não	Twitter	Site

44 O Twitter é a única plataforma que desenvolveu ferramentas *open source* para a detecção de *bots* - em grande medida, devido à ampla oferta de informações sobre usuários disponíveis na API do Twitter (metadados públicos), empregadas na construção de modelos de *machine learning* que classificam se as contas são controladas por *bots* ou humanos. Em outras plataformas, o rastreamento de *bots* é altamente dependente de análises e pesquisas realizadas manualmente, como a identificação de operações sobre-humanas (100 postagens/min, postagem de mensagens em intervalos regulares etc.). Num estudo sobre islamofobia às vésperas das eleições de meio de mandato dos EUA em 2018 na plataforma Gab, detectamos a presença de um *bot* de disseminação de desinformação a partir da identificação de postagens idênticas disparadas por um único usuário num intervalo curto de tempo.

Conclusão

Em última instância, todas as técnicas e ferramentas apresentadas neste guia servem para compor a abordagem adotada pelo usuário durante a coleta e a análise de dados. Usuários também deveriam considerar a possibilidade de desenvolver, a partir das técnicas demonstradas, um fluxo de trabalho e um sistema de armazenamento e estruturação dos dados coletados, potencialmente compartilhando as informações com as plataformas ou outros órgãos governamentais responsáveis. Diversos recursos apresentados ao longo do guia podem ser aplicados de acordo com as diferentes temáticas analisadas, seja em pesquisas sobre desinformação em contextos eleitorais ou sobre discursos de ódio e propaganda computacional presentes em manifestações políticas tradicionais na internet. Outro fator a ser considerado por analistas e pesquisadores é a disponibilidade de recursos - humanos, financeiros e técnicos – ao longo do desenvolvimento do projeto.

Mutas das ferramentas citadas são *open source*, mas outras são caras e difíceis de serem aplicadas sem conhecimento especializado sobre os recursos e os métodos envolvidos em sua concepção. Em diversos casos, é recomendável adotar soluções mais simples que podem ser postas em prática por pesquisadores menos experientes ou trabalhar colaborativamente com equipes multidisciplinares para que *insights* variados possam ser gerados a partir de uma mesma base de dados. Considere fomentar parcerias entre pesquisadores locais e especialistas internacionais para ampliar o escopo de *insights* e se dedique à construção de métodos para impulsionar a colaboração virtual entre comunidades, países e regiões.

Uma forma de angariar colaboradores, locais e internacionais, e unir esforços com as plataformas de mídia social para a realização de denúncias e pesquisas é por meio da rede Design 4 Democracy Coalition. A rede é uma parceria entre ONGs internacionais - como o NDI, o Instituto Republicano Internacional (International Republican Institute), a Fundação Internacional para Sistemas Eleitorais (International Foundation for Election Systems), o Instituto Internacional para Democracia e Assistência Eleitoral (International IDEA) e outras organizações da sociedade civil ao redor do mundo - e empresas de tecnologia, como Facebook, Microsoft e Twitter, visando à incorporação de princípios democráticos em sistemas, formas de moderação de conteúdo e políticas das plataformas de mídia social. Formas de análise e monitoramento *online* passaram a ser determinantes em eleições e democracias mundo afora, e este guia foi elaborado com o objetivo de oferecer as ferramentas, os métodos e as habilidades necessárias a grupos empenhados em lutar por esses ideais por meio de políticas e sistemas técnicos, contribuindo para o aprimoramento das informações que circulam na sociedade.

Abaixo, disponibilizamos mais referências, ferramentas *open source* e exemplos de código, além de um passo a passo para a utilização da API do Twitter.

Apêndice I: Exemplo de código de API - Coletando Dados nas APIs *Search* e *Streaming* do Twitter com o Pacote Rtweet

Nesta seção, vamos mostrar alguns exemplos de código para a coleta de dados históricos e em tempo real no Twitter. Com algumas poucas linhas de código, é possível coletar dados relevantes para o contexto eleitoral em análise. Uma vez agregados, os dados podem ser exportados para o formato CSV e posteriormente analisados no Excel ou no Google Sheets, ou então entregues a um cientista de dados encarregado pelo refinamento da análise. Mesmo ao analista que puder contar com um profissional especializado, é recomendável saber coletar dados em tempo real por conta própria. Por mais contraintuitivo que possa parecer, em análises de redes sociais, dados geralmente vão se tornando *mais* valiosos com o tempo, devido ao fato de capturarem desinformação, *bots* e ações e postagens efetuadas por atores nocivos potencialmente removíveis das plataformas por violação dos termos de serviço.

Passo 1: *Baixe o R, o RStudio e o Rtweet*

Neste guia, vamos ensinar como realizar a extração de dados básicos da API do Twitter utilizando a linguagem de programação R. Existe um pacote em R específico, chamado *rtweet*, que facilita enormemente a extração de dados do Twitter.

É necessário baixar e instalar determinados componentes antes de seguir em frente.

- Rstudio: https://www.rstudio.com/products/rstudio/download/
- R: https://www.r-project.org/

Passo 2: *Solicite acesso a uma aplicação do Twitter, receba a chave de acesso e crie um token*

A coleta de dados no Twitter é feita por meio de *aplicações* - esse é um meio seguro de utilizar uma conta pessoal para interagir com a plataforma por código. No passado, o Twitter disponibilizava as aplicações gratuitamente e sem restrições de acesso, mas, atualmente, é necessário que seja registrada uma aplicação, o que pode ser feito aqui.

Uma vez finalizado o credenciamento, é necessário efetuar o *login* no Twitter em algum navegador e acessar o site https://apps.twitter.com para obter as chaves do consumidor (*consumer keys*) e as chaves de acesso (*access keys*) - são quatro chaves no total. As chaves são *strings* de texto simples utilizadas pela aplicação para confirmar se os dados estão sendo solicitados, de fato, por uma pessoa - neste caso, o(a) leitor(a). O processo de utilização de chaves para *autenticação* é conhecido como *OAuth*, que significa "*open authorization*", ou "abrir (solicitar) autorização". Isso permite que as aplicações desempenhem ações na rede sem que os usuários sejam obrigados a transferir a senha e o nome de usuário a cada ação.

Após inserir as chaves e o nome da aplicação, utilize o código esboçado na janela a seguir para criar um "token" de requisição, que dará acesso à API do Twitter.

```
library(rtweet)
app<-"<app name here>"
consumer_key<-"<consumer key here>"
consumer_key_secret<-"<consumer key secret here>"
access_token<-"<access token here>"
access_token_secret<-"<access token secret here>"
create_token(app,consumer_key, consumer_key_secret, access_token, access_token_secret)
```

As linhas de código em R acima são linhas iniciais que podem ser utilizadas para autenticar a aplicação do Twitter e conectar à APÌ da plataforma. Uma vez autorizado o acesso, serão gerados os tokens de consumo e de acesso utilizados para a autenticação da aplicação (como ilustrado no código acima). Após a autenticação (i.e., quando o Twitter tiver computado que a aplicação está extraindo dados para o usuário logado, e não para terceiros), já é possível começar a interagir com a e extrair dados da API.

No site oficial do *rtweet* (aqui), também é possível encontrar um passo a passo detalhado do processo de autenticação, elaborado pelo Dr. Mike Kearney, professor da Universidade de Missouri e desenvolvedor do *rtweet*.

Capturando Dados Históricos:

Com o *rtweet*, é fácil capturar *tweets* utilizando uma *hashtag* ou um conjunto de *hashtags* de interesse na API Search do Twitter, que permite a coleta dos dados históricos, postados nos últimos 7-9 dias, correspondentes à consulta. Consultas são meramente critérios de interesse para a coleta dos *tweets* e podem conter *hashtags*, palavras-chave, nomes de contas, URLs, uma combinação dessas entidades ou todas juntas. Nesta seção, utilizaremos *hashtags* como exemplo, mas o processo e a sintaxe são exatamente iguais para as outras entidades.

O principal comando utilizado em pesquisas a *tweets* históricos é "*search_tweets()*".

```
my_data<-search_tweets("#ExampleHashtag", n=50000, retryonratelimit=TRUE)
```

Esta linha de código em R representa uma consulta à API Search do Twitter por até 50 mil tweets *contendo "*#ExampleHashtag*" ("hashtag ilustrativa") nos últimos 7-9 dias, e os resultados são salvos no* data frame *"my_data" ("meus dados"). Se a* hashtag *tiver sido usada menos de 50 mil vezes nesse intervalo de tempo, o número de* tweets *capturados será inferior. A alteração do valor de entrada de "n" provoca o aumento ou a redução do limite máximo de* tweets *consultados.*

```
multiple_hashtags<-search_tweets("#ExampleHashtag1 OR #ExampleHashtag2", n=50000, retryonratelimit=TRUE)
```

Esta linha de código em R representa uma consulta similar, mas estão sendo capturados até 50 mil tweets *contendo as* hashtags *"#ExampleHashtag1" ou "#ExampleHashtag2". Na API Search, a sintaxe pode ser utilizada para pesquisar mais de uma* hashtag. *No exemplo de código acima, os resultados são salvos no* data frame *"multiple_hashtags" ("múltiplas hashtags"). As* hashtags *são separadas pelos chamados "operadores booleanos": simplesmente "*AND*" ("E") e "*OR*" ("OU"). "*AND*" é usado para pesquisar* tweets *contendo as* hashtags *consultadas simultaneamente; "OR" é usado para pesquisar* tweets *contendo qualquer uma das opções de* hashtag *consultadas.*

Coletando Dados do Twitter em Tempo Real (*Streaming*):

A outra opção é coletar dados do Twitter em tempo real (*streaming*). Nesse tipo de consulta, é necessário especificar a quantidade de segundos desejada para a extração dos *tweets*, assim como as entidades pesquisadas (*hashtags*, URLs, palavras-chave, @-menções etc.).

A sintaxe para o *streaming* de *tweets* com o *rtweet* é um pouco diferente da utilizada em consultas à API Search. Na API de *streaming*, o comando utilizado é "*stream_tweets()*". Buscas por mais de um item devem ser separadas por vírgula.

```
my_streamed_data<-stream_tweets(q="#ExampleHashtag1",timeout=60)
```

```
my_streamed_data_w_multiple_hashtags<-stream_tweets(q="#ExampleHashtag1,#ExampleHashtag2",timeout=60)
```

*As janelas acima ilustram como utilizar o comando "*stream_tweets()*" do* rtweet *para extrair* tweets *em tempo real. No primeiro exemplo, a consulta se refere aos* tweets *contendo a* hashtag *"*#ExampleHashtag1*" num intervalo de 60 segundos. A única diferença do segundo exemplo é o acréscimo da* hashtag *"*#ExampleHashtag2*".*

Salvando os Resultados em um arquivo em formato CSV:

Na análise de dados, é muito comum utilizar arquivos em formato CSV ("*comma-separated values*", ou "valores separados por vírgulas"). Nesse tipo de formato, cada linha representa uma única fileira da planilha, e cada entidade entre vírgulas representa uma célula - ou, mais especificamente, um valor[45] dentro de uma célula. Um arquivo CSV é basicamente uma planilha num formato legível por máquina.

Os *tweets* salvos em formato convertido (CSV) já podem ser submetidos a uma análise mais rigorosa por um cientista de dados especializado ou analisados sem a ajuda de especialistas em um processador de planilha, como o Microsoft Excel ou o Google Sheets.

45 Em arquivos CSV e planilhas, "valores" também são denominados "campos".

```
write_as_csv(my_data,"my_data_as_a_csv_file.csv")
```

Esta linha de código em R utiliza o pacote rtweet *para converter o* data frame *de* tweets *"*my_data*" ("meus_dados") para o arquivo CSV "*my_data_as_a_csv_file.csv*" ("meus_dados_em_formato_csv.csv"). Uma vez convertidos, os dados podem ser facilmente compartilhados ou exportados para o Microsoft Excel e o Google Sheets.*

Considerações Finais

É extremamente recompensador saber salvar dados do Twitter em arquivos convertidos no formato CSV. Qualquer pessoa sem experiência em programação é capaz de aprender o processo descrito aqui em duas horas, ou provavelmente menos. A equipe de analistas que for capaz de armazenar dados relevantes do Twitter em formato CSV já está habilitada para realizar análises de dados relevantes sempre que for necessário.

Se o objetivo for armazenar os dados em longo prazo, é recomendável compactar o arquivo em formato .zip (ou em outro formato, como .tar), liberando espaço na memória e facilitando o compartilhamento do arquivo com outras pessoas e outros dispositivos.

Apêndice II: Ferramentas para OSINT

Inteligência de fontes abertas, comumente denominada de OSINT (*open source intelligence*), é a arte de investigar uma pergunta usando apenas informações ou dados disponíveis publicamente (ou "*open source*"). No contexto da desinformação e do monitoramento de redes sociais, esse tipo de pesquisa costuma ser acionado para expandir o leque de informações a respeito de atores nocivos ou suspeitos atuando na internet, incluindo contas falsas ou sites disseminadores de desinformação. Abaixo, segue uma lista com alguns recursos preciosos para aprender técnicas de OSINT.

- O site e o livro de Michael Bazzell:
  - https://inteltechniques.com
  - Open-Source Intelligence Techniques
- O kit de ferramentas de investigação online do portal Bellingcat: https://docs.google.com/document/d/1BfLPJpRtyq4RFtHJoNpvWQjmGnyVkfE2HYoICKOGguA/edit
- Lista pública de ferramentas de checagem e de OSINT, compilada pelo jornalista do BuzzFeed Craig Silverman: https://docs.google.com/document/d/1ZJbIUk5L8fe3VKK9CLVNMj9q0FdXG-RhQT6pyEgsS4I/edit
- O guia ComProp Navigator, publicado pelo Projeto de Propaganda Computacional do Instituto de Estudos da Internet da Universidade de Oxford (Computational Propaganda Project - Oxford Internet Institute, ou ComProp), é uma compilação de métodos e ferramentas para OSINT associados à desinformação e a outras pesquisas na internet: https://navigator.oii.ox.ac.uk/
- O guia *NewsGathering and Monitoring on the Social Web*[46], publicado pela First Draft: https://firstdraftnews.org/wp-content/uploads/2019/10/Newsgathering_and_Monitoring_Digital_AW3.pdf?x36710
- Fighting Disinformation Online: A Database of Web Tools, hosted by the Rand Corporation. https://www.rand.org/research/projects/truth-decay/fighting-disinformation.html
- O manual *Verification Handbook for Disinformation and Media Manipulation*[47]: https://datajournalism.com/read/handbook/verification-3/

46 "Captura e Monitoramento de Notícias na *Web* Social" em tradução livre.
47 "Manual para a Checagem de Desinformação e Manipulação da Mídia" em tradução livre.

Referências

Allcott, H., Gentzkow, M., & Yu, C. (2018). Trends in the Diffusion of Misinformation on Social Media. https://web.stanford.edu/~gentzkow/research/fake-news-trends.pdf

Borgatti, S., Everett, G., & Johnson, J. (2013). Analyzing Social Networks.

Democracy Reporting International. (October, 2019) *Guide for Civil Society on Monitoring Social Media During Elections.* https://democracy-reporting.org/wp-content/uploads/2019/10/social-media-DEF.pdf

Jack, C. (2017). *Lexicon of Lies.* Data & Society. https://datasociety.net/output/lexicon-of-lies/

Monaco, N. (2019). *Welcome to the Party: A Data Analysis of Chinese Information Operations.* Retrieved from https://medium.com/digintel/welcome-to-the-party-a-data-analysis-of-chinese-information-operations-6d48ee186939

National Democratic Institute. (May, 2019) *Disinformation and Electoral Integrity: A Guidance Document for NDI Elections Programs.* https://www.ndi.org/publications/disinformation-and-electoral-integrity-guidance-document-ndi-elections-programs

National Democratic Institute. (December, 2018). *Supporting Information Integrity and Civil Political Discourse.* https://www.ndi.org/publications/supporting-information-integrity-and-civil-political-discourse

Pakzad, R., & Salehi, Ni. (2019). Anti-Muslim Americans: Computational Propaganda in the United States. Institute from the Future. Retrieved from http://www.iftf.org/fileadmin/user_upload/downloads/ourwork/IFTF_Anti-Muslim_comp.prop_W_05.07.19.pdf

Russell, M., & Klassen, Mikhail. (2018). *Mining the social web.* Sebastopol, CA: O'Reilly Media.

Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making.* Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Woolley, S., Pakzad, R., & Monaco, N. (2019). *Incubating Hate: Islamophobia and Gab.* German Marshall Fund. http://www.gmfus.org/sites/default/files/publications/pdf/Incubating%20Hate%20-%20Islamophobia%20and%20Gab.pdf

Woolley, S., & Howard, P. (2017). *Computational Propaganda Worldwide: Executive Summary.* Working Paper. 2017.11. Oxford, UK: Project on Computational Propaganda. http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf

Zeiter, K., Pepera, S., Middlehurst, M., Ruths, D. (2019). *Tweets That Chill: Analyzing Online Violence Against Women in Politics.* National Democratic Institute. https://www.ndi.org/tweets-that-chill

NATIONAL
DEMOCRATIC
INSTITUTE

NDI.ORG