# Guia prático para a descodificação da desinformação.

Guião sistemático para a identificação das principais componentes de ataques de desinformação contra jornalistas e órgãos de comunicação social

# Guia Rápido

Aqui estão quatro passos que jornalistas, pesquisadores, e outros que estejam envolvidos na investigação de campanhas de desinformação contra a comunicação social devem tomar:

1. **Compreender o contexto**
2. **Analisar a cronologia, a plataforma e os métodos de disseminação**
3. **Identificar os actores envolvidos**
4. **Indicar as narrativas**

Este documento serve de um guião de que a de forma sistemática, se podem socorrer jornalistas e pesquisadores que realizam investigações sobre a desinformação e campanhas de difamação contra a comunicação social. É uma plataforma que permite identificar tácticas, técnicas e procedimentos (TTPs) usados para campanhas de desinformação. Nesse sentido, o guião procura prestar apoio aos esforços visando denunciar e contrariar tais campanhas, que têm sido usadas cada vez com mais frequência contra meios de comunicação social que se mostrem críticos, minando, dessa forma, a confiança pública sobre informação baseada em factos.

As directrizes constantes deste guião **não constituem um padrão universal**, dado que a desinformação continua a desenvolver-se com recurso a novas tecnologias. Este é um **documento contínuo**, que será actualizado à medida que novas tecnologias forem sendo desenvolvidas.

# 1 Compreender o contexto

**O objectivo aqui é compreender se, e como é que ataques de desinformação contra a comunicação social fazem parte de estratégias mais amplas visando minar a confiança pública ou promover narrativas específicas. Estes são os principais elementos que normalmente procuramos identificar:**

## Eventos e declarações relevantes dentro do período em que o ataque ocorre

Identificar o mais amplo contexto ou eventos que tenham contribuído para um determinado ambiente em que jornalistas são visados devido ao seu trabalho jornalístico. Essa informação pode estar ligada a eleições, movimentos de protesto ou crises ou desafios sociais (como por exemplo: imigração, questões sociais).

Identificar o tópico específico ou debate público que possa ter sido o motivo do ataque.

Identificar declarações proferidas por políticos, figuras públicas influentes ou outros actores políticos[1] que tenham criado o ambiente propício para legitimar ataques contra jornalistas.

## Contextos políticos e sociais relevantes

Identificar as agendas dos relevantes actores políticos ou outros relacionados com a campanha de desinformação.

Meios de comunicação social e canais de redes sociais com a tendência de disseminar falsas narrativas

Verificar plataformas digitais, assim como meios de comunicação social convencionais e não convencionais ou “alternativos”.

1 Actores políticos: pessoas directamente envolvidas em actividades político-partidárias ou na governação, incluindo: servidores públicos eleitos ou nomeados, que ocupem cargos políticos em qualquer ramo ou nível do governo; pessoas activas na vida político-partidária. Outros actores relevantes: figuras públicas que não estejam directamente envolvidas na vida política, mas que participem no debate público sobre tópicos relacionados com políticas.

# 2 Analisar a cronologia, a plataforma e os métodos de disseminação

**Pesquisadores e jornalistas devem estabelecer uma cronologia dos ataques como forma de melhor compreender o fluxo da campanha de desinformação. Para além disso, é preciso identificar as plataformas usadas para lançar a campanha, bem como os vectores que tornaram mais eficaz a sua disseminação, tais como hashtags, memes, vídeos/áudios e personificações (deepfakes) gerados através da Inteligência Artificial**

## Desenvolver uma cronologia sobre o ataque: Identificar e descrever os acontecimentos-chave que estejam relacionados com os ataques e criar uma cronologia

Em primeiro lugar, é necessário entrevistar a pessoa visada pela campanha, de modo a obter as primeiras informações sobre o ataque. Muitas vezes, Jornalistas visados têm um melhor entendimento sobre as componentes mais importantes de uma determinada campanha de desinformação e são capazes de descrever melhor o contexto, ajudando assim a desenhar uma cronologia inicial da campanha. Se a entidade visada é um órgão de comunicação social, recomenda-se que se fale com o respectivo pessoal: editores, jornalistas, gestores comunitários ou peritos em matéria de segurança digital.

Fazer nota da peça jornalística que terá sido causadora da campanha de difamação contra o jornalista ou órgão de comunicação social.

Notar quando e onde (plataformas, websites, etc.) os primeiros ataques foram registados e alistá-los cronologicamente. Ao assim proceder, descrever como é que durante o seu período de evolução, a campanha foi lançada em várias plataformas.

Alguns órgãos de comunicação social possuem arquivos permanentes sobre ataques e incidentes de assédio, portanto torna-se pertinente consultá-los e incluir todos os pormenores relacionados com o ataque que esteja a ser alvo de investigação.

## Identificar os canais de ataque e de assédio

Consulte redes sociais que contenham páginas e perfis que mencionem o indivíduo visado: Telegram, X, You Tube e Facebook são os mais comuns (pelo menos até 2024), mas verifique também o Instangram, Threads, Reddit, Tik Tok, WhatsApp e outras plataformas, dependendo da sua popularidade no contexto local.

Ataques e campanhas de assédio são muitas vezes levados a cabo através de meios de comunicação social "marginais", e websites que se fazem passar por meios de comunicação social convencionais (veja secção 3). Nos casos em que a origem destas plataformas não está clara, use dados disponíveis (registos oficiais, dados identitários de websites), para procurar determinar a natureza de propriedade e linha editorial.

## Identificar que elementos terão sido usados para a rápida propagação da campanha de difamação

Procure identificar hashtags, memes, imagens alteradas, vídeos, insultos, informação pessoal, personificações (deepfakes) de vídeo/áudio em várias plataformas.Tenha em conta que nem toda a postagem é por si só uma clara ameaça, portanto é importante registar também situações de ameaças veladas ou outras técnicas de intimidação tais como exposição (alguma parte de informação pessoal foi exposta, normalmente o email ou o número de telefone do jornalista visado) de modo a obter uma visão mais ampla das narrativas.

Procurar determinar se existe alguma litigância predatória (de má-fé) ou ameaças de processos judiciais ligados aos ataques.

Procurar determinar se o jornalista ou o órgão de comunicação social terá sido recentemente alvo de ataques cibernéticos.

Identificar comunicados de imprensa, declarações oficiais e conferências de imprensa protagonizadas por relevantes actores políticos ou outros.

**BOAS PRÁTICAS**

## Arquive os Localizadores Uniformes de Recursos (URLs) com todos os episódios de ataques ou falsas narrativas dirigidas ao visado.

Pode criar um Sistema interno de arquivo ou usar plataformas como https://ghostarchive.org/ ou https://archive.org/

# 3 Identificar os actores envolvidos

**Para os fins relacionados com a investigação, é importante identificar aqueles actores que tiverem instigado e/ou provocado o ataque e os que tiverem, de facto, o materializado. Estes actores podem ser figuras políticas, grupos de conversa, páginas, perfis anónimos, meios de comunicação social não convencionais e quaisquer outros actores relevantes ligados à campanha de desinformação.**

## Identificar e descrever os actores mais influentes que tiverem instigado a disseminação da campanha de desinformação

- Para cada actor político identificado, registar uma pequena biografia, filiação político-partidária ou de outra natureza, contas em redes sociais e seguidores e relevantes declarações.
- Procure identificar aqueles episódios em que estes actores tenham instigado os seus seguidores a atacar-em jornalistas.

## Identificar e descrever os principais actores de média (não convencional[2]) que tenham reportado favoravelmente sobre o ataque e apoiado as narrativas de desinformação

- Verificar os detalhes do proprietário do website e a conformidade do website face à legislação nacional em vigor.
- Notar a presença nas redes sociais, incluindo de seguidores.
- Verificar o arquivo de internet (Wayback Machine) para verificar interacções anteriores do website. Isto poderá revelar páginas "acerca" que tenham estado activas no passado, mas que foram removidas pelos administradores.
- Consultar bases de dados de media tais como Newsguard para mais informação.

2 Consideramos comunicação social não convencional (ou marginal) aquelas páginas da internet que se apresentam como parte dos media, mas que operam fora do âmbito do que chamamos de medias (ou meios de comunicação social) convencionais, e que muitas vezes no seu trabalho não se fazem vincular pelos padrões profissionais aplicáveis aos jornalistas. Muitas vezes eles não são transparentes em

BOAS PRÁTICAS

## Execute uma análise de infra-estrutura dos principais actores, bem como os websites envolvidos. Esta análise poderá exigir a necessidade de se juntar ao pessoal informático ou peritos OSINT, e poderá incluir, de entre outros:

- Análise DNS sobre os sites de propaganda
- Procura Inversa de Imagem (Reverse Image Searching) de logotipos, ícones ou imagens, de modo a rastreá-los a outras publicações
- Procura de domínio e IP

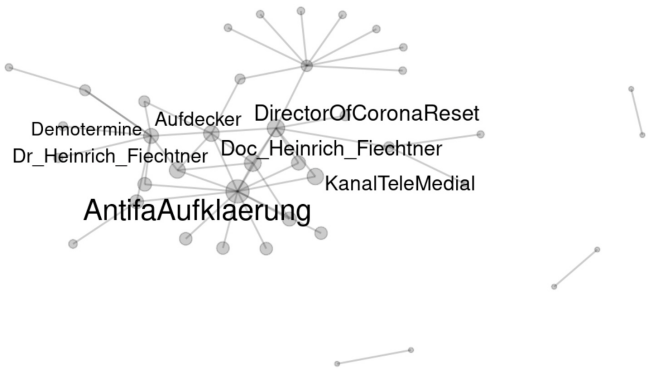
BOAS PRÁTICAS

## Execute uma análise de rede social, a fim de descobrir ligações e actores, assim como identificar até que ponto eles estão conectados

Um conjunto de ferramentas e empresas profissionais podem realizar este tipo de análises, ajustadas para as suas necessidades. Estas podem ser úteis na identificação de actores que não tenham sido encontrados na primeira busca, e têm a capacidade de mostrar a amplitude das mensagens relacionadas ao ataque. Aqui está uma lista dos softawres com que já trabalhamos:

- Gephi - The Open Graph Viz Platform
- NodeXL
- Gerulata
- Kivu.tech

**Exemplo:** procure familiarizar-se com a rede de canais em Telegram que partilharam mensagens intimidatórias contra um jornalista local na Alemanha.




Clique aqui para ver o relato completo.

# 4 Indicar as narrativas

**Identificar a narrativa específica que estiver a ser difundida pelo ataque de desinformação pode ajudar a revelar os objectivos por detrás da campanha.**

## Procurar estabelecer os factos atinentes às reivindicações que estiverem a ser feitas durante ataques

Identificar e estabelecer os factos sobre informação falsa usada no ataque contra um meio de comunicação social e a sua filiação política, financiamento ou informação organizacional.

É preciso ter em atenção que por vezes, campanhas de desinformação se referem a trabalhos anteriores dos jornalistas, e podem não estar estritamente relacionadas com o trabalho jornalístico específico que terá estado na origem da campanha de difamação.

## Identificação das narrativas de desinformação

Proceda a uma análise de conteúdo das publicações das redes sociais e artigos dos media e de discursos públicos.

Preste atenção às frases que tiverem sido usadas, prestar atenção a neologismos (nova terminologia que passa a ser usada frequentemente a partir de um determinado momento).

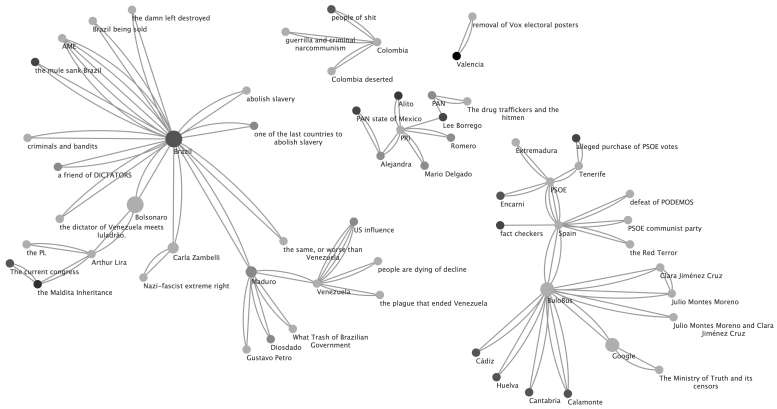
Usar o catálogo das narrativas de desinformação disponível na página do Observatório Europeu da Media Digital (EDMO) e estabeleça a ligação entre as suas constatações e as narrativas de desinformação existentes.

BOAS PRÁTICAS

## Crie redes de narrativas e rastreie estas falsas narrativas ao longo de um determinado período de tempo. Este tipo de análise proporciona uma visão geral sobre como é que narrativas contra os jornalistas estão interligadas e disseminadas nos mesmos canais e ao mesmo tempo, dando-lhe um entendimento mais consolidado sobre a amplitude da retórica.

A maior parte das ferramentas capazes de executar as redes de narrativas dependem da Inteligência Artificial. Neste caso, procure garantir a observância dos princípios de transparência quanto ao uso da tecnologia de Inteligência Artificial na redacção. Existem várias directivas, mas pode começar com a Parceria sobre os Princípios da Inteligência Artificial, que pode ser encontrada aqui.

**Exemplo:** Saiba mais sobre as redes de narrativas das teorias de conspiração disseminadas através dos canais do Telegram na Espanha.




Clique aqui para ler o document completo.

BOAS PRÁTICAS

## Produza um relatório sobre esta investigação. Ao seguir este guião será possível identificar as principais componentes de uma campanha de desinformação e dar resposta às principais questões jornalísticas: O quê? Quem? Porquê? Como? Quando? Onde?

Distribua o relatório pelas relevantes partes interessadas tais como associações de jornalistas ao nível nacional e internacional.

Antes disso, considere quaisquer riscos legais (por exemplo: fale com associações de jornalistas para aconselhamento jurídico ou com o departamento jurídico do seu próprio meio de comunicação social). Uma vez que os relatórios irão provavelmente indicar os indivíduos identificados como estando por detrás dos ataques, haverá a possibilidade de indivíduos ou empresas moverem processos judiciais por alegada difamação?

# Outros Recursos

## Amnistia Internacional: Laboratório de Evidências do Cidadão

"Este espaço digital visa apoiar organizações dos direitos humanos, pesquisadores, estudantes, jornalistas e outros para explorarem e partilhar métodos investigativos digitais disponíveis para pesquisa sobre direitos humanos."
Visite a página aqui.

## Pasta de Ferramentas de Investigação Online da Bellingcat

"Esta ferramenta investigativa aberta inclui orientações sobre serviços de satélite e mapeamento, ferramentas para a verificação de fotos e vídeos, websites para o arquivo de páginas web, e muito mais".
Visite o seu material aqui.

## Laboratório Digital de Investigação Forense

"O programa consiste de oficinas e sessões de formação prática abarcando literacia em comunicação social, técnicas de investigação em fonte aberta, verificação de factos e de fontes, análise de narrativas, observação de redes sociais, geolocalização, e muitos outros tópicos".
Visite as suas fontes e material aqui.

## Observatório Europeu da Media Digital (EDMO): Formações

"O EDMO disponibiliza de forma remota e regularmente, módulos de formação visando apoiar diversos intervenientes sobre como compreender e lidar com a desinformação online".
Visite os seus programas de formação aqui.

## Tactical Tech: Expondo o Invisível

"Expondo o Invisível aborda diferentes técnicas, ferramentas e métodos, a par de práticas individuais dos que trabalham nas novas fronteiras de investigação".
Visite a página aqui.

## Manual de Verificação para a Desinformação e Manipulação de Media, por Craig Silverman

"Este livro municiona os jornalistas com conhecimento para investigar contas de redes sociais, bots (robots), aplicações de mensagens privadas, operações de informação, personificações (deep fakes), bem como outras formas de desinformação e de manipulação dos media"
Descarregue o manual aqui.

## O projecto

# Descodificando o manual de desinformação do populismo na Europa

**O IPI, Taz, e Faktograf estão a colaborar na descodificação da propaganda populista na Europa, tendo como público-alvo verificadores de factos e jornalistas investigativos – ambos actores essenciais na luta contra a desinformação.**

*O projecto Descodificando o manual de desinformação do populismo na Europa conta com o apoio do Fundo Europeu para a Media e Informação (EMIF), gerido pela Fundação Calouste Gulbenkian.*

*Guia desenvolvido por Tajana Broz (Faktograf) e Javier Luque Martínez (IPI).*



*A tradução deste manual de apoio foi coordenada pelo Programa do IPI para África, em colaboração com o MISA Moçambique, e com o apoio do Gabinete do Governo do Canadá para os Direitos Humanos, Liberdades e Inclusão (OHRFI).*