WhatsApp nas eleições de 2018: o embate entre a lei, a tecnologia e o direito à privacidade

Por Miguel Freitas (02/02/2019)

Resumo

Para compreender o impacto do aplicativo WhatsApp nas eleições brasileiras de 2018 é necessário discutir não apenas as interações sociais que levaram esta plataforma a ganhar capilaridade e credibilidade a ponto de influenciar a opinião dos eleitores, como também os motivos técnicos e legais responsáveis pela incapacidade das instituições em coibir práticas consideradas indesejáveis, não democráticas e até mesmo francamente criminosas. Este artigo apresenta a situação atual, que muitas vezes é apenas superficialmente descrita por termos como "limbo jurídico", como sendo o resultado de um processo histórico e tecnológico movido por diferentes pressões, movimentos da sociedade e demandas de mercado. São discutidas ainda quais são as possibilidades que esta tecnologia oferece para que as instituições democráticas possam ser efetivas no cumprimento de algumas demandas da sociedade, particularmente visando coibir a prática de crimes e a manipulação dos processos eleitorais.

Introdução

Os aplicativos de comunicação segura utilizando criptografia fim-a-fim representam um empoderamento inédito do indivíduo em defender o seu direito à privacidade. Embora os conceitos legais de direito à privacidade e de proteção da intimidade remontem à discussões tão antigas quanto ao século XVII [1] ou antes, a capacidade de cumprimento destes direitos sempre dependeu, em alguma medida, da atuação das instituições. Benjamin Franklin, por exemplo, quando esteve a cargo das correspondências coloniais, exigiu um juramento de seus funcionários de que não abririam as cartas, o que somente foi tornado lei pelo congresso americano décadas depois, em 1782 [2].

Componente chave da revolução tecnológica atual, os algoritmos de criptografia seguros eram fortemente regulados, sendo considerados de uso militar e até mesmo proibidos de serem "exportados" pela legislação americana até 1992 [3]. Em um caso famoso, o professor e pioneiro da criptografia de e-mails Phil Zimmermann disponibilizou o código fonte do aplicativo PGP (Pretty Good Privacy) em servidores fora dos Estados Unidos em 1991, sendo então indiciado em uma investigação criminal [4]. Se a antiga lei de restrição de criptografia ainda estivesse em vigor, o WhatsApp não poderia ser desenvolvido em território americano, o que seria uma clara limitação à competitividade das empresas operando naquele país.

A grande inovação da solução de Zimmermann com o PGP foi de disponibilizar para qualquer usuário a possibilidade de criptografar os seus emails em seu próprio PC, com uma chave de criptografia tão segura que nem mesmo as agências de espionagem governamentais seriam capazes de decodificar o seu conteúdo. O e-mail criptografado só seria decodificado no PC do destinatário, isto é, uma criptografia fim-a-fim, imune à interceptações que possam ocorrer durante o trânsito da mensagem pela rede.

---

1 Daniel, Solove J. "A brief History of Information Privacy Law." Proskauer on privacy, GW Law Faculty Publication & Other Works, PLI (2006).

2 *Ibid*.

3 Radlo, Edward J. "Legal issues in cryptography." International Conference on Financial Cryptography. Springer, Berlin, Heidelberg, 1997.

4 Lauzon, Elizabeth. "The Philip Zimmerman Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues." Syracuse L. Rev. 48 (1998): 1307.

Embora esta tecnologia esteja, portanto, disponível de forma pública e gratuita desde 1991, diversos motivos explicam porque sua adoção ficou restrita a nichos tecnológicos ou de ativistas. A utilização do PGP não é simples e muitas vezes não é prática, exigindo um nível de conhecimento técnico, ou de procedimentos, que a maioria dos usuários não está disposta a assumir. Por algum tempo, o uso da criptografia pela população em geral parecia estar fadada a nunca acontecer, pois os usuários estariam dispostos a comprometer sua segurança em benefício da usabilidade. Riscos de segurança são frequentemente mal avaliados até a ocorrência de algum incidente mais grave.

A revolução das comunicações pela Internet produziu o pano de fundo perfeito para este incidente de segurança acontecer. Embora a interceptação telefônica e de correspondências continuasse formalmente regulada pela mesma legislação que protegia o direito à privacidade, exigindo procedimentos legais e autorizações judiciais para ser realizada, na prática os grandes nós da Internet se apresentavam como pontos de ataque irresistíveis à coleta indiscriminada de dados. A violação individual de todas as cartas enviadas pelo correio poderia ser, por si só, uma dificuldade operacional para qualquer estado que tentasse vigiar seus cidadãos. Por outro lado, o aumento da capacidade de processamento dos grandes computadores subitamente torna viável capturar todos e-mails que trafegam pela rede para análise posterior [5].

O incidente que produz uma virada na percepção mundial sobre abusos contra a privacidade pessoal teve origem no mesmo país que discutiu muitas de suas bases legais. O Caso Snowden, revelado pelo jornalista Glenn Greenwald [6] em 2013, mostrou como a tecnologia estava permitindo que o estado burlasse mecanismos legais de proteção pessoal e monitorando indiscriminadamente todos os seus cidadãos, ações que até então pareciam restritas a estados totalitários e ditaduras. A grande repercussão e a compreensão das implicações deste caso motivaram o desenvolvimento de diferentes soluções tecnológicas, inclusive por este autor [7], visando rebalancear o jogo. Isto é, prover mecanismos para que os cidadãos possam se defender do abuso de estados que não respeitem seus direitos individuais. Na sequência dos mesmos eventos, o governo brasileiro transforma em prioridade a aprovação da lei conhecida como Marco Civil da Internet [8], trazendo como pedra fundamental o princípio da privacidade.

Diferentes aplicativos de mensagens instantâneas ganharam popularidade com a disseminação dos “smart phones” nos anos recentes. Para destacar três dos mais relevantes atualmente, WhatsApp, Telegram e Signal foram lançados, respectivamente, em 2009, 2013 e 2014. Ao contrário dos dois últimos, o WhatsApp não tinha como apelo inicial a característica de fornecer criptografia fim-a-fim. É preciso reconhecer que foi provavelmente uma decisão comercial, movida por pressão dos concorrentes pós-Snowden e de uma demanda de mercado, que leva o WhatsApp a finalmente adotar este recurso para todos usuários em 2016. No caso particular do Brasil, a adoção em larga escala do WhatsApp é explicada também, e principalmente, pela cobrança de taxas de envio de SMS pelas operadoras de celular. Esse movimento leva o WhatsApp a construir uma base de usuários desproporcionalmente grande no país, contabilizando 120 milhões de usuários ativos em 2018 [9], ou cerca de 57% da população brasileira.

---

5 Assange, Julian, Jacob Applebaum, Andy Müller-Maguhn, and Jérémie Zimmermann. “Cypherpunks - liberdade e o futuro da Internet”. Boitempo Editorial, 2013.

6 Greenwald, Glenn. “No place to hide: Edward Snowden, the NSA, and the US surveillance state”. Macmillan, 2014.

7 Freitas, Miguel. "Twister: the development of a peer-to-peer microblogging platform." International Journal of Parallel, Emergent and Distributed Systems 31.1 (2016): 20-33.

8 Agencia Brasil. “Após denúncias de espionagem, governo pedirá agilidade na votação do Marco Civil da Internet.”, 08/07/2013. Disponível em: <http://memoria.ebc.com.br/agenciabrasil/noticia/2013-07-08/apos-denuncias-de-espionagem-governo-pedira-agilidade-na-votacao-do-marco-civil-da-internet>

9 Folha de S. Paulo. “Facebook chega a 127 milhões de usuários mensais no Brasil”, 18/07/2018. Disponível em: <https://www1.folha.uol.com.br/tec/2018/07/facebook-chega-a-127-milhoes-de-usuarios-mensais-no-brasil.shtml>

A arquitetura de segurança do WhatsApp

A implementação da criptografia fim-a-fim na plataforma WhatsApp foi anunciada oficialmente em 2014 em parceria com a empresa “Open Whisper Systems” [10] do aplicativo Signal, sendo concluída em 2016. Embora o WhatsApp seja um aplicativo de código fechado, o protocolo escolhido possui especificação pública [11], permitindo que pesquisadores possam, de certa forma, atestar formalmente a segurança da solução adotada [12]. Isto é, excluindo-se a possibilidade de “*bugs*” ou “*backdoors*” inseridas propositalmente no código, considera-se que o WhatsApp garante a privacidade da comunicação de seus usuários, uma vez que nem mesmo a própria empresa teria acesso ao conteúdo das mensagens trocadas. O protocolo de segurança possui ainda recursos avançados como a possibilidade de verificar, em um encontro pessoal entre dois usuários, se as chaves de segurança dos dispositivos não foram adulteradas em trânsito [13].

Existe, no entanto, um conjunto de informações que não são protegidas pela criptografia fim-a-fim e que seriam teoricamente passíveis de monitoramento pela empresa, os chamados registros de uso ou metadados. Em outras palavras, o WhatsApp pode alegar que não é capaz de descobrir “o que você fala”, mas é capaz de saber “com quem você conversou”.

Há motivos plausíveis por trás da decisão de projeto que permite à empresa WhatsApp conhecer os registros de uso dos usuários. Em primeiro lugar, se os servidores do WhatsApp têm como missão realizar a entrega das mensagens de um remetente para um destinatário, é tecnicamente muito mais fácil implementar uma arquitetura de roteamento que execute esta tarefa quando os metadados são conhecidos. Há também a motivação de se evitar a multiplicação de “spams”, o que poderia minar a confiança na plataforma. Para isso o WhatsApp utiliza análises estatísticas e de comportamento dos usuários, sempre utilizando como base os metadados, conforme declarações da própria empresa [14].

A existência e o armazenamento dos dados de acesso e da atividade dos usuários é amparada ainda em duas evidências públicas: os Termos de Uso do Serviço WhatsApp, que em seu item 7 fala do armazenamento dos "logs" [15], e em uma investigação conduzida pela revista Forbes que analisou o histórico de processos judiciais da empresa, encontrando diversos casos em que esta forneceu metadados para investigações do FBI [16].

A contribuição do autor para este debate foi uma pesquisa própria demonstrando que cada mídia (foto, áudio ou vídeo) compartilhada na plataforma produz um arquivo criptografado que é então hospedado em um servidor web (HTTP) da companhia. Ainda que o conteúdo deste arquivo seja protegido por criptografia fim-a-fim, a existência desta URL, sua criação e seus acessos geram metadados que indubitavelmente são de conhecimento da empresa. Tendo ainda como objetivo preservar o desempenho da ferramenta, o WhatsApp optou por não criptografar novamente este arquivo a cada novo encaminhamento, mantendo as chaves de criptografia originais e apenas encapsulando a URL em uma nova mensagem. São estas as características técnicas de funcionamento da plataforma que nos permitem afirmar que o WhatsApp poderia identificar a origem de uma determinada mídia a

10 Techcrunch. “WhatsApp Partners With Open WhisperSystems To End-To-End Encrypt Billions Of Messages A Day”, 18/11/2014. https://techcrunch.com/2014/11/18/end-to-end-for-everyone/

11 Wikipedia. “Signal Protocol is a non-federated cryptographic protocol that can be used to provide end-to-end encryption for voice calls, video calls, and instant messaging conversations”. https://en.wikipedia.org/wiki/Signal_Protocol

12 Cohn-Gordon, Katriel, et al. "A formal security analysis of the signal messaging protocol." Security and Privacy (EuroS&P), 2017 IEEE European Symposium on. IEEE, 2017.

13 WhatsApp Inc. “WhatsApp Encryption Overview - Technical white paper”, 19/12/2017. https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

14 Techcrunch. “How WhatsApp is fighting spam after its encryption rollout”, 02/02/2017. https://techcrunch.com/2017/02/02/how-whatsapp-is-fighting-spam-after-its-encryption-rollout/

15 WhatsApp’s Terms of Service, Privacy Policy, https://www.whatsapp.com/legal/#privacy-policy

16 Forbes. “Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops”, 22/01/2017. https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/

partir de seu identificador único ou URL. Ou seja, é teoricamente possível, caso haja interesse da empresa em colaborar com a justiça, descobrir a identidade do primeiro remetente de uma mídia compartilhada no WhatsApp.

O caso WhatsApp nas eleições brasileiras de 2018

O embate entre a justiça brasileira e o WhatsApp tem sido reportado com relativa frequência na mídia. Em um caso que gerou bastante repercussão em 2016 uma juíza decidiu pela suspensão da operação do aplicativo em todo o Brasil, por entender que a empresa não estava colaborando adequadamente com uma determinada investigação [17]. Muitas destas disputas decorrem do desconhecimento das instâncias legais a respeito do funcionamento da plataforma WhatsApp com relação aos seus recursos de segurança e criptografia. O novo equilíbrio entre instituições públicas, empresas de tecnologia e usuários empoderados com criptografia parece ter tornado algumas práticas legais obsoletas. Ademais, a sociedade não parece disposta a abrir mão deste empoderamento e tende a ficar do lado das empresas na garantia da inviolabilidade de suas comunicações pessoais, ao menos nos casos em que a alternativa oferecida tem sido a suspensão total dos serviços.

Nas eleições de 2018 alguns eventos merecem destaque dentro embate. Uma decisão da justiça eleitoral de 12/10/2018 negou pedido do Partido dos Trabalhadores (PT) para remover conteúdos caluniosos e falsos de grupos de WhatsApp [18]. O argumento utilizado pelo ministro, de que os grupos representariam um espaço privado e, portanto, não sujeito ao controle exercido pela justiça em páginas públicas na Internet é questionável. A maioria destes grupos oferecem convites públicos para ingresso de novos membros sem necessidade de autorização explícita dos administradores. Desta forma, cabe questionar: se qualquer usuário pode entrar no grupo através de uma URL, o que diferencia este grupo de um fórum aberto de discussões na Internet? Diferenças tecnológicas entre plataformas seriam suficientes para mudar o entendimento legal sobre a natureza pública/privada destes espaços?

Também em outubro de 2018 uma denúncia mostrou empresários bancando disparos de mensagens em massa contra o PT [19]. A prática, ilegal por incluir doações de campanha não declaradas por empresas e também por utilizar bases de usuários não autorizadas, pode ter influenciado o resultado das eleições na opinião de alguns especialistas [20]. Na sequência da denúncia o próprio WhatsApp divulgou nota afirmando ter bloqueado contas associadas aos disparos ilegais [21]. O bloqueio admitido pela empresa provavelmente foi resultado de uma análise interna mais rigorosa de metadados armazenados anteriormente, a partir dos indícios apresentados na reportagem original da Folha.

O Tribunal Superior Eleitoral tentou obter em determinação de novembro de 2018 a lista dos empresários e candidatos que teriam pago pelos disparos em massa. O WhatsApp negou ter sido contratado pelo candidato para este fim e não apresentou respostas [22]. O episódio evidenciou duas

17 Globo/G1. “WhatsApp: Justiça do RJ manda bloquear aplicativo em todo o Brasil”, 19/07/2016. http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-deve-ser-bloqueado-decide-justica-do-rio.html

18 TSE. “TSE nega pedido do PT para remover conteúdo de grupo no WhatsApp”, 12/10/2018. http://www.tse.jus.br/imprensa/noticias-tse/2018/Outubro/tse-nega-pedido-do-pt-para-remover-conteudo-de-grupo-no-whatsapp

19 Folha de S. Paulo. “Empresários bancam campanha contra o PT pelo WhatsApp”, 18/10/2018. https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml

20 O Estado de S. Paulo. “TSE ignorou dimensão do problema, diz consultor de campanha de Alckmin”, 20/10/2018. https://politica.estadao.com.br/noticias/eleicoes,tse-ignorou-dimensao-do-problema-diz-consultor-de-campanha-de-alckmin,70002555305

21 Jornal Nacional/G1. “WhatsApp bloqueia contas e investiga empresas suspeitas de integrar esquema que visava a caluniar candidato do PT”, 19/10/2018. https://g1.globo.com/politica/eleicoes/2018/noticia/2018/10/19/whatsapp-bloqueia-contas-e-investiga-empresas-suspeitas-de-integrar-esquema-que-visava-a-caluniar-candidato-do-pt.ghtml

22 Folha de S. Paulo. “Twitter, Facebook e WhatsApp não respondem principais perguntas sobre seu papel na eleição brasileira”, 13/11/2018. https://www1.folha.uol.com.br/poder/2018/11/twitter-facebook-e-whatsapp-nao-respondem-principais-perguntas-sobre-seu-papel-na-eleicao-brasileira.shtml

atuações disfuncionais deste processo: diversas perguntas formuladas pelo TSE não faziam sentido tecnicamente, assim como também a pouca disposição do WhatsApp em colaborar com este tipo de investigação.

Em novembro de 2018 este autor ofereceu denúncia à Procuradoria Geral da República (PGR) com indícios que poderiam ser usados para identificar os criados de diversos conteúdos falsos ("fake news") que circularam nos grupos políticos do WhatsApp no período eleitoral. Para tal, foram analisadas mensagens coletadas por outros pesquisadores em 277 grupos, identificando as postagens que possuíam as melhores características de rastreabilidade. O critério utilizado foi destacar, dentre os conteúdos de mídia mais populares, aqueles que seriam comprovadamente falsos e que preservassem a mesma URL criptografada original por grandes períodos de tempo, mesmo aparecendo em grupos diferentes. Para avançar nesta linha investigativa, a Polícia Federal deveria solicitar ao WhatsApp, mediante ordem judicial, informações sobre o usuário e/ou endereço IP responsável pelo "upload" do arquivo para os servidores da companhia. A iniciativa foi destacada em matéria da Folha de S. Paulo [23] mostrando que aparentemente a PF não se interessou por seguir esta linha.

Em resposta oficial, o WhatsApp negou armazenar os registros de "upload" de arquivos que permitiriam a identificação do criador dos conteúdos de mídia [24]. A resposta do WhatsApp é problemática do ponto de vista legal, pois a empresa estaria possivelmente infringindo o artigo 15 do Marco Civil [25] que exige que provedores de aplicação guardem tais registros pelo prazo de 6 meses, sendo obrigados a fornecê-los somente por determinação judicial.

Na opinião deste autor, e também de outros especialistas consultados, o mecanismo de rastreio aqui sugerido oferece uma janela segura para investigações moderadas, isto é, sem permitir abusos e o acesso em massa pelo Estado. Isto se aplicaria também a investigações de diferentes naturezas não eleitorais como, por exemplo, crimes de pedofilia. É necessário avançar com este debate na sociedade, reestabelecendo limites e deveres das empresas de tecnologia para que estas possam colaborar efetivamente com investigações legítimas sem violar os direitos individuais.

23 Folha de S. Paulo. "Relatório enviado à PF sugere caminho para rastrear fake news", 17/01/2019. https://www1.folha.uol.com.br/poder/2019/01/relatorio-enviado-a-pf-sugere-caminho-para-rastrear-fake-news.shtml

24 Folha de S. Paulo. "WhatsApp nega ter registros que possam levar aos disseminadores de fake news", 23/01/2019. https://www1.folha.uol.com.br/poder/2019/01/whatsapp-nega-ter-registros-que-possam-levar-aos-disseminadores-de-fake-news.shtml

25 Presidência da República, Lei Nº 12.965 de 23 de abril de 2014. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

WhatsApp, política mobile e desinformação: a hidra nas eleições presidenciais de 2018

WhatsApp, mobile politics and misinformation: the Hydra of Brazil's 2018 presidential election

WhatsApp, política móvil y desinformación: la hidra en las elecciones presidenciales de 2018

João Guilherme Bastos dos Santos
Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INCT-DD).
E-mail: santos.jgb@gmail.com.

Miguel Freitas
Centro de Estudos de Telecomunicações da PUC-Rio. E-mail: miguel@cpti.cetuc.puc-rio.br.

Alessandra Aldé
Universidade Estadual do Rio de Janeiro (UERJ). E-mail: ale3alde@gmail.com.

Karina Santos
Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INTC-DD)
E-mail: karinasantos93@hotmail.com.

Vanessa Cristine Cardozo Cunha
Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INTC-DD). E-mail: vanessa_cardozo07@hotmal.com.

RESUMO
Iniciamos esta pesquisa a dez meses das eleições executivas de 2018, período no qual investigamos o comportamento coletivo de 90 grupos de WhatsApp interconectados e de apoio aos seis principais presidenciáveis, bem como os mais de 500 mil textos e imagens enviados pelos usuários, por meio dessa ferramenta, durante os cinco meses de campanha eleitoral. Com este estudo, identificamos que o alcance ampliado do aplicativo se dá através da viralização de mensagens como consequência direta da interconexão estrutural entre esses grupos. Neste cenário, confirmamos nossas hipóteses sobre a importância das características e das topologias da rede para uma compreensão aprofundada sobre a desinformação em larga escala via WhatsApp. Como resultado, reconhecemos quais métricas da rede são bem sucedidas na previsão e caminhos preferenciais para a circulação da desinformação segmentada e possibilidades de rastreio de fontes originais das notícias.
Palavras-chave: WhatsApp. Viralização. FakeNews. Eleições presidenciais 2018; *Mobile instant messaging services*.

ABSTRACT
Starting ten months before the 2018 presidential election, this paper analyses the collective behaviour of 90 interconnected WhatsApp groups supporting six different candidates, and more than 500 thousand texts and images sent during five campaign months. Large scale reach in the application relies on its counterintuitive viral spread, a direct consequence structural interconnection among groups. It confirms the importance of network topologies and characteristics in any serious understanding of WhatsApp large scale misinformation. We identified which network metrics are successful in predicting preferential pathways for segmented misinformation.
Keywords: WhatsApp. Viral spread. FakeNews, 2018 presidential election campaign. *Mobile instant messaging services*.

RESUMEN
Iniciamos esta investigación a diez meses de las elecciones ejecutivas de 2018, período en el cual investigamos el comportamiento colectivo de 90 grupos de WhatsApp interconectados y de apoyo a los seis principales presidenciables, así como los más de 500 mil textos e imágenes enviados por los usuarios, a través de esa herramienta durante los cinco meses de campaña electoral. Con este estudio, identificamos que el alcance ampliado de la aplicación se da a través de su viralización contra-intuitiva, consecuencia directa de la interconexión estructural de esos grupos. Por lo tanto, confirmamos nuestra hipótesis sobre la importancia de las características y las topologías de la red para una comprensión en profundidad sobre la desinformación a gran escala a través de WhatsApp. Como resultado, reconocemos qué métricas de la red tienen éxito en la previsión y caminos preferenciales para la circulación de la desinformación segmentada
Palabras clave: WhatsApp. Viralización. FakeNews. Elecciones presidenciales 2018. *Mobile instant messaging services*.

Submissão: 25-2-2019
Decisão editorial: 24-5-2019

1. Introdução

O WhatsApp mantém um design de rede privada com criptografia ponta-a-ponta, mas as estruturas de rede decorrentes de suas apropriações sociais no Brasil o transformaram em uma poderosa ferramenta de difusão de informações para grandes públicos. Como alternativa aos serviços de SMS pagos, a possibilidade de serviços de mensagens *mobile* sem custos de internet atraiu um contingente grande de pessoas que não têm acesso à rede de outro modo, ajudando o aplicativo a alcançar a marca de 120 milhões de usuários ativos em 2018. Se os *sites* de *fact-checking* exigem acesso à internet paga e muitas organizações jornalísticas restringem o acesso aos seus produtos, campanhas políticas souberam utilizar esta conjuntura a seu favor espalhando desinformação com viés eleitoral em momentos chave.

Um caso emblemático ocorreu às vésperas das eleições presidenciais de 2014, quando a notícia falsa de que Alberto Youssef foi envenenado durante sua prisão na Superintendência da Polícia Federal em Curitiba viralizou por WhatsApp atingindo *smartphones* do país inteiro menos de 24 horas antes do pleito. Uma montagem colocava a manchete no portal de notícias G1, acompanhada pelo rumor de que haveria envolvimento do Partido dos Trabalhadores no

crime supostamente para impedir uma delação de Youssef. O rumor foi desmentido publicamente pela Polícia Federal brasileira e pelo G1, e sua circulação foi condenada pelo Ministro da Justiça, mostrando a preocupação de diversos atores com as consequências desta mentira em um cenário eleitoral acirrado e polarizado – mas não havia como dar uma resposta proporcional na mesma velocidade ou retirar a montagem que circulava por mensagens privadas.

O impacto deste tipo de estratégia teria potencial muito maior em 2018. De acordo com *Digital News Report*[1] entre 2014 e 2018 o uso de *smartphones* para consumo de notícias cresceu de 35% para 65% enquanto a utilização de computadores passou de 64% para 62%. O uso do Facebook para notícias caiu 17 pontos entre 2016 e 2018 enquanto o WhatsApp cresceu alcançando a marca de 46%. Autoridades e comentaristas, no entanto, subestimaram consideravelmente o potencial estrago da apropriação do aplicativo repetindo e multiplicando, de modo muito mais sistemático e eficaz, a dinâmica do 'caso Youssef'. Esta possibilidade faz com que a campanha no WhatsApp – ainda cara devido a cobranças 'por envio' – comece a ser economicamente mais interessante às campanhas eleitorais.

Crescimentos súbitos na adesão a mensagens específicas são tema de investigações em torno de ações coletivas que antecedem a internet. Propostas explicativas giram em torno da ideia de cooperação condicional, em que diferentes fatores – visibilidade do comportamento, pressão por pares, percepção sobre viabilidade da ação, quantidade de pessoas

[1] Disponível em: < http://www.digitalnewsreport.org/survey/2017/brazil-2017/ > Acesso em: junho de 2018.

envolvidas, traços de personalidade – aumentariam subitamente a quantidade de adesões a partir de um limiar, massa crítica ou ponto de virada relacionados a um destes fatores. A premissa comum é, portanto, que as escolhas das pessoas muda de acordo com informações sobre quantas outras pessoas participam de determinada ação coletiva (SCHELLING, 1978; GRANOVETTER, 1978).

Apropriações de dispositivos com acesso à internet conferem nova potência a esta dinâmica. De ações em larga escala coordenadas sem a existência de organizações centrais (BIMBER et al, 2012) e o súbito crescimento em escala relativamente independente de lideranças centralizadas (MARGETTS et al, 2015), colocam em evidência pautas políticas que fogem à tutela de seus produtores iniciais – trazendo ao debate termos como *organização sem organizações* ou *liderança sem líderes*, respectivamente. Há ainda a ação conectiva (plataformas digitais como fundamento da organização política na forma de redes de compartilhamento de narrativas pessoais) (BENNETT E SEGERBERG, 2012) e a relevância de elementos narcisistas na adesão a ações com alta visibilidade em redes *online* (PAPACHARISSI, 2010). Revisões sobre internet e mudanças abruptas na escala de apoiadores em ações coletivas (MARGETTS et al, 2016) apontam a relevância da interação entre visibilidade e informação social (e seus desdobramentos em termos de constrangimento, aprovação, pressão etc.) juntamente com variações em traços de personalidade na guinada abrupta no número adesões.

A viralização em larga escala e recorrente de mensagens políticas em campanhas no WhatsApp contraria todas estas chaves explicativas. O aplicativo

não possui perfis públicos localizáveis por busca, algoritmos de impulsionamento de visibilidade, agregação automática de informação social ou entrega direcionada de conteúdo. Pelo contrário, limita o número de encaminhamentos diretos e o número de pessoas que podem pertencer a cada grupo, descartando elementos considerados peças chave na viabilidade de viralizações rápidas e recorrentes em plataformas como Facebook. A viralização de uma notícia falsa exige um aumento exponencial de visibilidade a cada encaminhamento, incompatível com índices normais de compartilhamento individual em redes de contatos privados. É neste ponto que os grupos de WhatsApp dedicados à política, em geral segmentados, com mais de duzentas e cinquenta pessoas cada e canais de comunicação entre si, entram em cena. Propomos que a utilização de métodos de análise de redes complexas pode elucidar a possibilidade de viralização neste cenário. Este artigo se diferencia, portanto, das análises de conversações que caracteriza a produção aindaincipiente sobre novas especificidades relacionadas aos aplicativos de mensagens instantâneas por celular (Mobile Instant Messaging Services) (VALERIANI E VACCARI, 2018).

Associado a criptografia, a possibilidade de viralização torna-se uma poderosa arma para estratégias criminosas. Por isso sua apropriação é previsível, mantendo a fonte relativamente segura e tornar difícil seu rastreamento, escondida do escrutínio público geral, mas em contato com o segmento alvo em particular. A segmentação é uma possibilidade mesmo que o aplicativo não ofereça estes dados: em um modelo mais sofisticado, pode ser feita por algoritmos que cruzam dados de diferentes redes *online*, superan-

do déficits em dados de qualquer uma destas redes tomada individualmente; em modelos mais simples, cruzando números de celular e CEPs presentes *online* – possibilitando segmentação geográfica por rua e inferências demográficas –, através de páginas militantes que divulgam links para grupos de WhatsApp em redes visíveis como o Facebook (possibilitando registros sobre perfil das páginas e grupos associados, além de fazer com que estes links possam ser achados por ferramentas de busca), entre outros. Ao replicar conteúdo de modo dificilmente rastreável e anonimizando a fonte, o WhatsApp da um passo adiante em relação a ferramentas como *dark posts* e *microtargeting*, utilizados para difundir informações para nichos específicos enquanto as mantém ocultas do escrutínio público no Facebook.

Como apontado por estudos sobre crescimentos abruptos em escala de campanhas políticas (MARGETTS *et al*., 2015), a identificação de traços específicos de personalidade pode indicar maior ou menor propensão a compartilhar conteúdos, possibilitando seleção de pontos com maior probabilidade de gerar o que chamamos de viralização. O caso extremo do escândalo com a Cambridge Analytica mostra que dados sobre traços de personalidade podem ser inferidos a partir de informações de comportamento *online* registradas por *sites* de redes sociais. Os chamados robôs podem atuar, portanto, identificando nichos e enviando mensagens regularmente, utilizando a propensão destes nichos a compartilhar um tipo específico de informação ao mesmo tempo em que cria uma aparência de campanha orgânica.

É importante frisar que a apropriação visando difusão de desinformação criminosa e cripto-

grafada é uma distorção específica e reprimível, e que os aplicativos de comunicação segura utilizando criptografia fim-a-fim também podem ser uma ferramenta importante na defesa do direito à privacidade. A inovação da criptografia fim-a-fim está em permitir que qualquer usuário possa criptografar suas mensagens em seu próprio celular com uma chave de criptografia segura, protegendo-o até mesmo de agências de espionagem governamentais, que dificilmente seriam capazes de decodificar o seu conteúdo. A mensagem criptografada é decodificada apenas no dispositivo do destinatário, ficando assim imune a interceptações que possam ocorrer durante o seu trânsito pela rede. Esta mesma dinâmica, no entanto, exige medidas específicas para evitar ações criminosas como a viralização sistemática de notícias falsas com finalidade de manipulação eleitoral.

Apesar de esta tecnologia estar disponível de forma pública e gratuita desde 1991 (LAUZON, 1998), diversos motivos explicam porque sua adoção ficou restrita a nichos tecnológicos ou de ativistas. O Caso Snowden, revelado pelo jornalista Glenn Greenwald em 2013, mostrou como a internet estava sendo utilizada para burlar mecanismos legais de proteção pessoal e monitorar indiscriminadamente cidadãos americanos e estrangeiros (GREENWALD, 2014; MIGUEL, 2016). Esse evento chamou a atenção para a necessidade de prover mecanismos para que os cidadãos possam se defender do abuso de Estados que não respeitem seus direitos individuais. Na sequência dos mesmos eventos, o governo brasileiro transforma em prioridade a aprovação da lei conhecida como Marco Civil da Internet, trazendo como pedra fundamental o princípio da privacidade.

Diferentes aplicativos de mensagens instantâneas ganharam popularidade com a disseminação dos "*smart phones*" nos anos recentes. Para destacar três dos mais relevantes atualmente, WhatsApp, Telegram e Signal foram lançados, respectivamente, em 2009, 2013 e 2014. Ao contrário dos dois últimos, o WhatsApp não tinha como apelo inicial a característica de fornecer criptografia fim-a-fim. Foi provavelmente uma decisão comercial, movida por pressão dos concorrentes pós-Snowden e de uma demanda de mercado, que leva o WhatsApp a finalmente adotar este recurso para todos usuários em 2016.

Ainda em 2017, uma série de entrevistas com profissionais de internet e campanha política (SANTOS E NEHRER, 2017), apontavam expectativas de profissionais familiarizados com a pauta das notícias falsas com o uso do WhatsApp em 2018. Juntamente com pesquisas anteriores sobre utilização de redes sociais *online* por apoiadores de Bolsonaro (ALDÉ E SANTOS, 2012; SANTOS E CUNHA, 2014), estas entrevistas foram utilizadas como base para o desenvolvimento de metodologias específicas capazes de analisar o uso do WhatsApp para disseminar informações falsas e definir quais dinâmicas tornam possível a viralização neste ambiente opaco.

A apropriação bem-sucedida do WhatsApp por apoiadores de Jair Bolsonaro resulta da cooperação de diversos grupos – incluindo eleitores – e um conhecimento específico voltado para viralização sistemática de conteúdo. A compreensão deste fenômeno exige uma alteração no modo como este aplicativo é analisado, superando obstáculos colocados por seu design voltado para troca de mensagens privadas,

através do cruzamento de dados, composição de redes e análises de fluxo de conteúdo.

Tendo em vista esses aspectos fundamentados em estudos prévios sobre o campo, testamos quatro hipóteses envolvendo a desinformação em larga escala via WhatsApp, durante as eleições presidenciais, são estas:

> (H1) Pessoas presentes em mais de um grupo podem viabilizar uma estrutura de grupos interconectados no WhatsApp, fazendo com que o aplicativo esteja sujeito a lógicas de rede bipartite e tornando possível que a desinformação se viralize rapidamente. O que propomos não é que esta seja uma característica a priori no aplicativo, mas um resultado da estrutura de rede contingente resultante de opções pessoais de usuários ao distribuírem-se em grupos;
> (H2) Usando métricas de algoritmos de rede, poderíamos encontrar correspondências entre a centralidade das redes e a relevância dos grupos nesse processo assimétrico, avançando, assim, em nossa análise sobre a ampliação viral da desinformação;
> (H3) Trata-se de um processo variante no tempo, que pode ser separado em estágios/encaminhamentos, no qual a desinformação vai dos nós centrais para os periféricos, ampliando exponencialmente por meio do encaminhamento de grupos.
> (H4) Acreditamos que haja indícios do difusor inicial nas mensagens viralizadas, hipótese cujo teste se beneficia da identificação dos grupos em que esta informação falsa foi circulada primeiro em decorrência da confirmação das hipóteses anteriores – possibilitando parcerias com esferas dedicadas ao aperfeiçoamento da legislação sobre campanhas políticas e a responsabilização dos possíveis produtores profissionais envolvidos.

2. H1: WhatsApp como uma rede bipartite

Com base na recomposição de redes e análise da estrutura de grupos pudemos testar a hipótese norteadora da presente análise: mais do que uma rede de pessoas conectadas através de grupos, o WhatsApp está sujeito à dinâmicas de uma rede *bipartite* de grupos interconectados por participantes em comum[2] que regulam o intercâmbio de informações, permitem o aumento exponencial de visibilidade e lógicas de difusão viral de notícias falsas mesmo dentro de uma rede fechada (H1). Essa rede de grupos mantém um fluxo de informações criptografado, opaco ao escrutínio público e intenso em períodos eleitorais. Transitando rapidamente em diferentes grupos, essas notícias podem fomentar ondas de compartilhamento que invadem novas levas de grupos a cada etapa, fluxo passível de mapeamento a partir da aplicação de métodos de constituição estrutural e análise de redes.

Metodologicamente, esta constatação tem desdobramentos relevantes. Primeiro, para além de propriedades *topológicas*, a análise de redes reconhece propriedades *dinâmicas* de viralização e contágio. As limitações de visibilidade e tamanho de grupos afastam o WhatsApp do modelo de rede que caracteriza o Facebook – *preferential attachment/scale free*, em que atores bem conectados possuem uma vantagem cumulativa, atraindo mais conexões e concentrando centralidade –, aproximando-o de modelos descentralizados. Menos centralizado, este modelo de rede apresenta maior resistência a ataques ou desativação de *nós/grupos* (ALBERT E BARABÁSI, 2000) em compa-

[2] Uma rede bipartite, ou seja, uma rede em que grupos não estão formalmente associados entre si, mas em que participantes em comum podem constituir conexões e fomentar dinâmicas de rede.

ração ao Facebook, o que significa que a retirada de grupos do ar por decisão judicial afeta pouco a dinâmica da rede. Isso não impede que, via de regra, uma pessoa esteja intencionalmente presente em um número grande de grupos.

Em ambientes políticos polarizados, esse modelo baseado em vários grupos separados pode levar a composição, intencional ou não, das chamadas *redes policêntricas segmentadas e integradas* (GERLACH, 2001). Entre as inovações desta estrutura destacam-se as funções adaptativas ou comportamento de Hidra: o alcance a diversos núcleos sociais devido a diferenças entre os perfis sociais, culturais, táticos de cada grupo da coalizão, bem como às funções assumidas; impossibilidade de repressão centralizada, uma vez que a independência e autonomia entre os grupos fazem com que a destruição de um destes não interrompa o comportamento global da rede e que para cada grupo neutralizado surja um novo com funções semelhantes; a possibilidade de reorganização e compensação, uma vez que a falha de um grupo não necessariamente implica falha dos demais, o que permite um aprendizado coletivo por tentativa e erro sem que o coletivo de grupos precise incorrer em erro. A integração dialoga com a composição de identidade por antagonismo, dedicada à utilização de *gatilhos emocionais* capazes fomentar coesão interna ao grupo, muitas vezes através do incentivo à hostilidade contra atores externos (MCDERMOTT, 2011).

A viralização nesse cenário acontece porque o aumento no estabelecimento de conexões torna mais provável que pessoas de grupos diferentes estabeleçam pontes, levando a um aumento abrupto na quantidade de pessoas indiretamente conectadas

cada vez que um novo grupo ou conjunto de grupos se conectam. Limites para a quantidade de pessoas em cada grupo potencializam a segmentação que caracteriza esta dinâmica. Esse comportamento não linear conduz a um ponto de guinada em que os vértices passam abruptamente a estar conectados ao chamado *componente gigante*, identificado em três sistemas naturais: difusão de doenças epidêmicas em redes de contato físico, redes neurais e problemas de rede de matriz genética (RAPOPORT E HORVATH, 1961).

O modelo serve tanto para entender a composição da estrutura da rede, quanto para analisar a dinâmica de circulação de informação viral nesta estrutura, embora estas duas dinâmicas obedeçam a critérios de expansão diferentes. Utilizamos esta abordagem como alternativa à ideia de viralização associada a algoritmos de visibilidade e limiares de ação política (MARGETTS *et al*., 2015) entendendo que uma lógica similar de crescimento acelerado após determinado limiar está associada a um limiar da *estrutura* da rede, e o crescimento na *quantidade* é um efeito colateral – e não a causa – do aumento abrupto no número de elementos atingidos pela viralização.

Essa questão traz a possibilidade de (H2) desenvolver métodos voltados para as redes que rapidamente identificam quais grupos estão mais propensos a estar no *início* do processo de viralização, bem como os (H3) caminhos preferenciais para desinformação *segmentada*, pontos cruciais que impedem a propagação desses conteúdos e que retardam o processo viral, podendo torná-lo inviável.

Todos os testes empíricos feitos pelo grupo de pesquisa em Tecnologias da Comunicação e Política (TCP) da UERJ confirmaram esta possibilidade (H1). Ini-

ciando suas conexões a partir da entrada em grupos de WhatsApp em apoio a candidatos e segmentos diferentes (incluindo Jair Bolsonaro, Fernando Haddad, Ciro Gomes, Marina Silva, Geraldo Alckmin e Henrique Meirelles) em maio, os sete pesquisadores do TCP envolvidos no experimento terminaram conectados ao mesmo *componente gigante*. Na rede formada por 9.812 perfis distribuídos em 90 grupos de WhatsApp especializados em campanha e discussão política, 99,11% dos perfis – independentemente de viés político – formam um *componente gigante*, comprovando a viabilidade de dinâmicas virais.

A descentralização também foi confirmada, afastando-se de dinâmicas de redes como Facebook (a distribuição de grau indica que 8.354 perfis estão em apenas um grupo, 1.107 em dois, 225 em três, 81 em quatro, 23 em cinco, 10 em seis, 9 em sete dois em 8 grupos e um em 16). A possibilidade de circulação de links, no entanto, conecta os dois modelos de rede, permitindo a usuários do Facebook a distribuição de links para grupos de WhatsApp (com entrada condicionada ao limite de membros) e perfis do WhatsApp a distribuição de links para postagens do Facebook, canalizando a participação dos membros, promovendo ondas de comentários, curtidas ou ataques súbitos sem que a atuação dos grupos que promoveram esta onda seja visível. Os links entre grupos também são utilizados para ataques, em que links de convite são jogados em grupos adversários para entradas em massa seguidas por ondas de xingamento e conteúdo impróprio ou ainda em que adversários se passam por apoiadores que precisam se tornar administradores para poder adicionar amigos ao grupo e assim que

conseguem esta função mudam o nome do grupo invertendo apoios, alteram foto e excluem membros.

3. H2 e H3: Viralização (sem algorítimo de visibilidade ou informações sociais) e o papel das métricas de rede

Reconhecer o caráter viral destas dinâmicas exige a aceitação de duas premissas, cujos desdobramentos metodológicos são relevantes para compreensão do uso político do WhatsApp. Primeiro, viralização implica *direcionalidade* (relações assimétricas entre uma fonte e seus destinatários) e um processo *variável no tempo* cuja progressão pode ser avaliada em etapas (e em que destinatários em uma etapa podem se tornar fontes na etapa seguinte). Isso coloca a questão: como identificar rapidamente que grupos têm mais chances de estar no início deste processo? Este é o ponto vulnerável da rede, uma vez que impedir a propagação a partir destes pontos desacelera e pode inviabilizar viralização.

Essa abordagem é especialmente útil em casos de redes criptografadas como o WhatsApp, cujas características podem ser válidas para compreender os modelos de rede (considerando algumas inferências sobre os *padrões* que ocorrem fora de nossa amostragem). Isso é particularmente interessante num cenário no qual a ausência de um número total de grupos que integram globalmente essa rede proíbe métodos que dependam de proporções quantitativas ou representativas. A primeira consequência importante do reconhecimento dessa assimetria é que os grupos não são equivalentes e, portanto, a simples coleta e quantificação de seus conteúdos ignora as funções estruturais da rede. Esse erro, combinado com a fal-

ta de mensuração da representatividade nessa rede privada, pode inviabilizar qualquer generalização de conclusões quantitativas.

Assim, nossos critérios para entrar em grupos segmentados, de apoio aos seis candidatos anteriormente mencionados e já ativos no início de 2018, ocorreram através do acesso a links em páginas favoráveis a esses presidenciáveis no Facebook. Por meio desses links, fomos automaticamente adicionados a outros grupos especializados durante o período pré-eleitoral, o que nos permitiu obter análises que variam conforme o tempo. Sobre esse aspecto, vale ressaltar que considerar o tempo também é relevante na análise das redes, dado que os perfis não podem visualizar informações postadas no grupo antes de suas entradas.

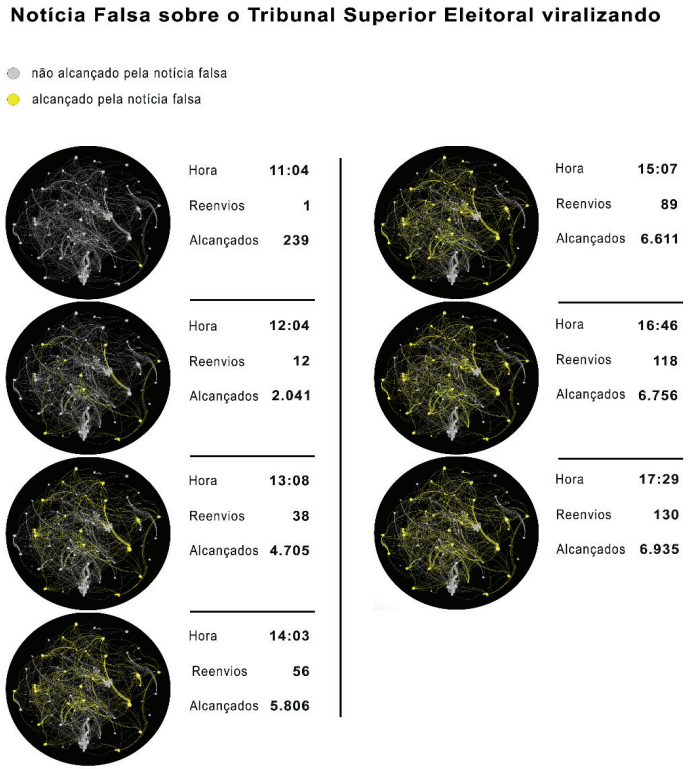
A posição estrutural de cada grupo define sua relevância neste processo: se para circular por diversos pontos da rede uma informação necessariamente passa por um grupo, este grupo tem um nível de *centralidade* nesta rede, aumentando quando outros grupos centrais passam a estar conectados graças a este grupo em particular (*eigenvector*, medida que varia entre 0 para grupos sem centralidade e 1 para grupos com centralidade máxima). Isso também faz com que as informações cheguem com mais probabilidade a este grupo, e aumente suas chances de viralização a partir do momento em que o alcança. A criptografia da fonte e impedimentos de acesso a conteúdos anteriores à entrada do perfil em um grupo deixa as possibilidades de análise deste fenômeno restritas a pesquisadores que já estivessem acompanhando quando o fenômeno ocorreu, capazes de cruzar estes dados com informações sobre estrutura da rede.

A imagem a seguir mostra a viralização de uma notícia falsa sobre o Tribunal Superior Eleitoral na rede descrita acima, atingindo 6.935 dos 9.812 perfis em poucas horas – aglomerados de pontos cinza indicam grupos sem contato com a notícia, amarelos aqueles que tiveram contato com ela e as linhas apontam conexões entre eles. A notícia afirma que o Tribunal Superior Eleitoral teria informado a anulação de 7,2 milhões de votos e que 2 milhões teriam sido necessários para que Bolsonaro vencesse no primeiro turno. A viralização por compartilhamento traz a possibilidade de analisar as etapas de difusão e encontrar a fonte inicial e o papel de cada grupo neste processo. Entre os dez primeiros a receber a notícia falsa viralizada, seis possuíam centralidade maior do que 0,90; dois acima de 0,85; e os restantes com centralidade 0,69 e 0,64. Entre os dez últimos a receber a notícia, três têm centralidade inferior a 0,18; quatro entre 0,52 e 0,42; e os três restantes possuem centralidades de 0,60, 0,73 e 0,85. Acusações contra o TSE foram uma constante entre apoiadores de Jair Bolsonaro e são sugeridas pelo próprio candidato em sua primeira declaração a jornais após o resultado do primeiro turno. Das 438,4 mil mensagens textuais coletadas nesta rede entre junho e outubro de 2018, 3.348 envolviam 'urnas' e o TSE, a maior parte delas falsa.

Ao identificar *padrões* estruturais de conexão e fluxo, modelos de rede permitem utilizar uma escala reduzida da rede para projetar e compreender a dinâmica da rede em seu todo. Esta abordagem é *impositiva* uma vez que não é possível visualizar a rede 'completa' de grupos de WhatsApp e estabelecer qualquer parâmetro de representatividade ou fidedignidade para métodos de *quantificação* simples.

Uma vez que delimitamos nossa rede, o aumento na quantidade de pessoas alcançadas desacelera nas etapas finais a despeito da continuidade de compartilhamentos. No cenário real, em que a difusão segue para outros grupos periféricos fora da rede analisada, esta desaceleração levaria muito mais tempo.

Figura 1



Fonte: autores.

Portanto, a notícia progride preferencialmente *de* grupos com maior centralidade *para* grupos pe-

riféricos – numa lógica policêntrica, quando outros grupos centrais são atingidos a dinâmica se repete, propagando a viralização. A cada etapa, a multiplicação faz com que a quantidade de informações replicadas para o próximo conjunto de grupos seja exponencialmente maior do que a anterior. Para fora da rede de grupos dedicados/especializados em política, grupos mais difundidos socialmente como de família e outras afinidades, tendem a ser atingidos. Isso faz com que a simples *quantificação* de tipos de grupos em que a notícia falsa pode ser encontrada, como os 'de família', sem levar em consideração sua *centralidade* na rede que promoveu a viralização, conduza a erros graves na atribuição de relevância, *invertendo* completamente a lógica da rede. Embora sejam mais numerosos e conjuntamente possam ter um número maior de *eleitores*, a presença de notícias falsas em grupos periféricos é a *consequ*ência e não *causa* da difusão sistemática de uma notícia falsa específica. É justamente a ignorância em relação a este processo que faz alguns apoiadores assumirem que "se eu não recebi para compartilhar este conteúdo, ninguém recebeu e sua difusão é orgânica", sem questionar quem as produziu/difundiu *antes* de seu contato com a notícia.

Vale frisar que, entre os grupos que receberam a desinformação repetidamente, também pudemos identificar padrões confirmando nossa proposta: entre os dez grupos com maior número de repetições essa informação aparece em média 8,6 vezes, a centralidade menor é 0,84 e a centralidade média é 0,92 – 6 de dez grupos de centralidades são superiores a 0,90. Número médio de membros do grupo é 234. Por outro lado, entre os grupos de dez grupos que receberam

apenas uma vez, a centralidade média é de 0,38 e os membros médios do grupo é 97,25.

Confirmando H2, o uso de algoritmos para identificar comunidades estruturadas considerando apenas a *topologia* de rede para identificar comunidades estruturadas (algoritmo de modularidade) foi bem sucedido em agrupar automaticamente os apoiadores de diferentes partes em diversas categorias, identificando subgrupos entre os defensores do mesmo candidato e também categorizando redes de discussão política com nenhum candidato específico – com erros de categorização raros envolvendo grupos de discussão sem candidato específico. Isso mostra que a heterogeneidade entre os atores envolvidos, e que essas diferenças podem ser vistas na estrutura da rede, incluindo diferenças entre aqueles que apoiam o mesmo candidato. Apesar de identificar subgrupos no apoio dos candidatos, separando-os, o algoritmo não agrupou os apoiadores de diferentes candidatos – com a exceção mencionada acima.

Nossa análise do caso envolvendo TSE também indica que houve viés de preferência partidária na circulação desta notícia. Ela foi compartilhada 202 vezes (retornando a circulação depois do último registro nos grafos), mas a despeito das interconexões entre os 90 grupos, só 41 são atingidos: 37 são grupos de apoio a Bolsonaro entre conservadores, 'de direita' ou pró-militares, e quatro são de discussão política sem candidato definido. A preferência por um candidato pode indicar um maior ou menor filtro ao compartilhamento de notícias específicas pelos perfis que conectam grupos favoráveis a este candidato a outros grupos da rede.

Reconhecidos os caminhos preferenciais e a dinâmica favorecida por grupos segmentados mais dispostos a compartilhar, entendemos que a viralização no WhatsApp envolve ao menos três etapas: primeiro a etapa de produção e difusão inicial; em seguida sua circulação em grupos segmentados dedicados a política, interconectados por membros mais dispostos a compartilhá-la e inseri-la em uma dinâmica de viralização; e por fim grupos periféricos não dedicados a política, quantitativamente mais numerosos, embora proporcionalmente irrelevantes na etapa mais intensa da viralização. Ao se aproximar de grupos com maior centralidade (*eigenvector*) tendemos a nos aproximar da fonte primária da notícia falsa.

Esse tipo de percepção ajuda a elucidar as dificuldades encontradas pelos jornalistas e comentaristas na tentativa de entender o papel do WhatsApp em *Outubro*, como uma reação à participação eleitoral: *(i)* eles não podiam entrar em grupos políticos que já alcançavam o limite dos participantes, *(ii)* quando os grupos não estavam lotados, os jornalistas dependiam de links de convite presentes fora do WhatsApp, em um cenário de ataques recíprocos que faziam com que muitos grupos políticos restringissem seus convites de links para listas de encaminhamento internas; *(iii)* quando finalmente conseguiram fazer parte de um grupo, nenhum comentário anterior a sua entrada podia ser visualizado. Esses profissionais da mídia, então, se depararam com uma série de filtros sobre qualquer conteúdo disponível, tendo apenas acesso a mensagens de novos grupos com links postados fora do WhatsApp – em geral, esses grupos não estavam preocupados com "estrangeiros" e não possuíam muitos membros.

4. H4 - A arquitetura de segurança do WhatsApp, rastreamento e o caso brasileiro em 2018

O potencial das pesquisas efetivadas no auxílio da compreensão destes casos paralelamente aos desencontros entre funcionamento da tecnologia e as iniciativas legais motivaram, em novembro de 2018, a denúncia encaminhada à Procuradoria Geral da República (PGR) com indícios que poderiam ser usados para identificar os criadores de diversos conteúdos falsos ("*fake news*") que circularam nos grupos políticos do WhatsApp no período eleitoral. Para tal, foram analisadas mensagens utilizadas no teste das hipóteses anteriores, já divulgadas em diferentes congressos acadêmicos (SANTOS et al, 2018a; SANTOS et al, 2018b), identificando as postagens que possuíam as melhores características de rastreabilidade.

Primeiro destacamos, dentre os conteúdos de mídia mais populares, aqueles que seriam comprovadamente falsos e que preservassem a mesma URL criptografada original por grandes períodos de tempo, mesmo aparecendo em grupos diferentes. A identificação bem-sucedida no âmbito acadêmico aponta a possibilidade de que órgãos competentes solicitarem ao WhatsApp, mediante ordem judicial, informações sobre o usuário e/ou endereço IP responsável pelo "upload" do arquivo/notícia falsa para os servidores da companhia.

O material resultante desse teste e enviado a autoridades competentes é composto por dois documentos: (1) parecer técnico demonstrando o funcionamento da plataforma, os limites impostos pela criptografia fim-a-fim e o tipo de informação que pode ser solicitado à empresa de forma tecnicamente plausível. (2) listagem de conteúdos falsos/caluniosos

com detalhamento de sua propagação nos grupos monitorados e seus identificadores únicos (*hashes* e URLs) que deveriam ser solicitados pela justiça.

Para produzir esta listagem de conteúdos de mídia rastreáveis, o primeiro passo consiste em agrupar as imagens e vídeos por similaridade visual, de forma automatizada. É comum, principalmente no caso de vídeos, que várias versões do mesmo conteúdo circulem na rede, diferindo apenas em termos de qualidade ou resolução de imagem.

Entre os achados, destacamos: qualquer modificação no conteúdo do arquivo, por menor que seja, produz um identificador *hash*[3] – tipo de identificador único que é gerado, utilizando uma função matemática, a partir do conteúdo do arquivo – completamente diferente. Dois *hashes* são encontrados dentro da plataforma WhatsApp, o *hash* do arquivo de mídia original e o *hash* do arquivo criptografado. Por motivos técnicos e de segurança, cada vez que o arquivo é criptografado, obtém-se um resultado diferente e, portanto, um *hash* diferente. Isto conduz a segunda variabilidade frequentemente encontrada nas mensagens de WhatsApp: um mesmo arquivo original enviado (por upload e não por encaminhamento) à rede por diferentes usuários produz versões criptografadas diferentes, com diferentes *hashes* correspondentes. A observação deste padrão de propagação permite discriminar casos em que o conteúdo original foi inicialmente distribuído por outra plataforma, por exemplo, via Facebook. Quando diferentes usuários baixam o arquivo do Facebook para então retrans-

[3] No WhatsApp os *hashes* são sempre calculados por meio do algoritmo SHA256 e codificados com BASE64.

miti-lo, de forma independente, dentro do WhatsApp é produzido um padrão diferente.

É possível perceber que em alguns casos, apesar de o *hash* da mídia (arquivo jpg) ser igual em todas as mensagens mostradas, o *hash* do arquivo criptografado (arquivo enc) apresenta versões diferentes e, para cada uma delas, o WhatsApp produziu uma URL diferente. Esta URL pode ser digitada em um *browser*, permitindo que qualquer pessoa possa fazer o *download* do arquivo criptografado caso este ainda esteja na rede. O arquivo, no entanto, somente será decodificado no conteúdo original de posse das chaves de criptografia que são encaminhadas na própria mensagem e restritas aos emissores e destinatários do arquivo.

Em casos de elevada possibilidade de que esse conteúdo tenha sido distribuído originalmente em outra plataforma, casos marcados por várias URLs não são considerados casos de boa rastreabilidade. Não seria produtivo encontrar os diferentes usuários que fizeram a cópia de uma plataforma para a outra, pois – apesar de a prática ser igualmente problemática – não há nenhum indicativo de que estes teriam qualquer relacionamento com o criador original do conteúdo.

Nesse ponto, a identificação de casos de viralização interna no WhatsApp são relevantes. Eles indicam casos em que praticamente todos os encaminhamentos se referem ao mesmo *hash* de mídia original – devido à lógica viral – e também a mesma URL (e consequentemente o mesmo *hash* criptografado). Um caso de boa rastreabilidade nesse sentido é a suposta mensagem entre Gabrielli e Fernando Haddad combinando a publicação de uma "bomba"

na Folha. Foram encontradas centenas de mensagens encaminhadas com a mesma URL, o que nos leva a concluir que o conteúdo é originário da própria plataforma WhatsApp e compartilhado quase exclusivamente por meio da opção de "encaminhamento" oferecida e ativando lógicas virais de difusão. Se o WhatsApp fornecesse às autoridades o IP responsável pelo upload desta URL poderíamos chegar ao usuário criador deste conteúdo.

Em resposta oficial, porém, o WhatsApp nega armazenar os registros de *upload* de arquivos que permitiriam a identificação do criador dos conteúdos de mídia. A resposta do WhatsApp é problemática do ponto de vista legal, pois a empresa estaria possivelmente infringindo o artigo 15 do Marco Civil que exige que provedores de aplicação guardem tais registros pelo prazo de seis meses, sendo obrigados a fornecê-los somente por determinação judicial.

O mecanismo de rastreio aqui sugerido oferece uma janela segura para investigações moderadas, isto é, sem permitir abusos e o acesso em massa pelo Estado. Isto se aplicaria também a investigações de diferentes naturezas não eleitorais como, por exemplo, crimes de pedofilia. É necessário avançar com este debate na sociedade, reestabelecendo limites e deveres das empresas de tecnologia para que estas possam colaborar efetivamente com investigações legítimas sem violar os direitos individuais.

Considerações finais

A pesquisa conseguiu confirmar empiricamente quatro hipóteses: o WhatsApp está sujeito a lógicas de uma rede bipartite graças a sua estrutura de grupos segmentados interconectados e métricas podem

identificar grupos centrais neste processo variante no tempo através de diferentes etapas. De etapa em etapa, a desinformação vai de nós centrais para nós periféricos ampliando seu alcance exponencialmente e se tornando viral. O cruzamento entre centralidade (*eigenvector*) e identificação de comunidades estruturadas (*modularidade*) oferece um mecanismo automatizado de detecção de rotas preferenciais para difusão de notícias virais em cada comunidade ou coalizão de comunidades encontrada na rede. Replicar a utilização deste algoritmo em um número maior de redes pode avançar estabelecendo *modelos de rede*.

Identificando caminhos iniciais das notícias e características específicas nas *hashes* agregadas aos encaminhamentos no aplicativo, podemos explorar quais possibilidades esta tecnologia oferece para que instituições democráticas possam ser efetivas no cumprimento de algumas demandas da sociedade, particularmente visando coibir a prática de crimes e a difusão de notícias falsas por meio de recursos técnicos disponíveis.

Referências

ALBERT, Réka; BARABÁSI, Albert-László. **Topology of evolving networks: Local events and universality**. Phys. Rev. Lett. 85. 2000, p. 5234-5237.

ALDÉ, Alessandra; SANTOS, João Guilherme Bastos dos. **Petições Públicas e batalhas digitais**. XXI COMPÓS, Juiz de Fora (MG), 2012.

BENNETT, W. Lance, SEGERBERG, Alexandra. *The Logic of Connective Action*. Information, **Communication & Society**, vol. 15, no 5, p. 739-768, 2012.

BIMBER, Bruce, FLANAGIN, Andrew J, STOHL, Cynthia. **Collective Action in Organizations: Interaction and Engagement in an Era of**

Technological Change. Cambridge University Press, 2012.

FREITAS, Miguel. "*Twister: the development of a peer-to-peer micro-blogging platform.*" **International Journal of Parallel, Emergent and Distributed Systems** 31.1 (2016): 20-33.

GERLACH, Luther. The structure of social movements: environmental activism and its opponents In: ARQUILLA, John, RONFELDT, David. **Networks and netwars**: The future of terror, crime, and militancy. RAND, 2001.

GRANOVETTER, Mark. Threshold Models and Collective Behavior. American**. Journal of Sociology**, 83, pp. 1420-1443, 1978.

GREENWALD, Glenn. "No place to hide: Edward Snowden, the NSA, and the US surveillance state". Macmillan, 2014.

LAUZON, Elizabeth. "The Philip Zimmerman Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues." **Syracuse L. Rev**. 48 (1998): 1307.

MARGETTS, Helen; JOHN, Peter; HALE, Scott A.; Yasse Ri, Taha. **Political Turbulence: How Social Media Shape Collective Action**. Princeton e Oxford: Princeton University Press, 2016.

MCDERMOTT, Rose. Emotional Manipulation of Political Identity. In: Le Cheminant, Wayne; Parrish, John M (org.). **Manipulating Democracy.** Routledge, 2011.

PAPACHARISSI. Zizi A. **A Private Sphere**: Democracy in a Digital Age. Cambridge: Polity Press, 2010.

RAPOPORT A, e HORVATH, W. A study of a large sociogram. **Behavioral Science** 6. 1961, p. 279-291.

SANTOS, João Guilherme Bastos dos.; SANTOS, Karina; CARDOZO, Vanessa . **Cartografia do Whatsapp**: a rede de apoio aos presidenciáveis nas eleições de 2018. In: 3'Congresso Nacional de Estudos Comunicacionais da PUC, 2018. Minas - Poços de Caldas: Conec, 2018a.

SANTOS, João Guilherme Bastos dos; SANTOS, Karina; CARDOZO, Vanessa. La red del 'mito' 2018: Articulaciones políticas de grupos de extrema derecha en Whatsapp. Conferência Latinoamericana de Ciências Sociais, 2018. Buenos Aires, Argentina: CLASCO, 2018b.

SCHELLING, Thomas. **Micromotives and Macrobehavior**. New York: Norton, 1978.

VALERIANI, Augusto, VACCARI, Cristian. Political talk on mobile instant messaging services: a comparative analysis of Germany, Italy, and the UK. Information, **Communication and Society,** vol. 21, no 11, pp. 1715-1731, 2018.

João Guilherme Bastos dos Santos
Doutor em Comunicação Social pela Universidade do Estado do Rio de Janeiro (UERJ), pesquisador vinculado ao Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INCT-DD) alocado no grupo Tecnologias da Comunicação Política. E-mail: santos.jgb@gmail.com.

Miguel Freitas
Recebeu seu B. E., M. Sc. e doutorado em engenharia elétrica pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), em 2002, 2004 e 2011, respectivamente. Atua como engenheiro de pesquisa no Centro de Estudos de Telecomunicações da PUC-Rio. E-mail: miguel@cpti.cetuc.puc-rio.br.

Alessandra Aldé
Doutora em Ciência Política pelo Instituto Universitário de Pesquisa do Rio de Janeiro, professora de Comunicação Política da Universidade Estadual do Rio de Janeiro (UERJ), coordenadora do grupo de pesquisa Tecnologias da Comunicação Política. E-mail: ale3alde@gmail.com.

Karina Santos
Mestranda em Comunicação Social pela Universidade Federal Fluminense (UFF), pesquisadora do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-RIO), membro do Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INTC-DD) alocado no grupo Tecnologia da Comunicação Política. E-mail: karinasantos93@hotmail.com.

Vanessa Cristine Cardozo Cunha
Mestre em Comunicação Social pela Universidade Estadual do Rio de Janeiro (UERJ), doutoranda do Programa de Pós Graduação em Comunicação Social da UERJ, membro do Instituto Nacional de Ciência e Tecnologia em Democracia Digital (INTC-DD) alocado no grupo Tecnologia da Comunicação Política. E-mail: vanessa_cardozo07@hotmal.com.

Sala de Atendimento ao Cidadão - MPF 20190028040

MPF Sistema Cidadão <manifestacao-noreply@mpf.mp.br>
To: miguel@cpti.cetuc.puc-rio.br

Wed, Apr 24, 2019 at 4:53 PM

Sala de Atendimento ao Cidadão — MPF Ministério Público Federal — Seu direito, nosso dever.

Ilmo(a) Sr.(a) **MIGUEL DE ANDRADE FREITAS**,

Resposta à manifestação nº **20190028040** (22/04/2019).

Agradecemos o contato com este canal de comunicação e informamos que sua manifestação foi recebida sob nº PR-SP-00044139/2019 e encaminhada à Divisão Cível Extrajudicial da Procuradoria da República no Estado de São Paulo.

Agradecemos o contato por este canal de comunicação.

Sua Manifestação continuará em atendimento no MPF sob o número **PR-SP-00044139/2019**. A partir de agora, o seu andamento poderá ser consultado no Portal de Transparência do MPF, pelo link:

Consultar Documento (disponível em até 24 horas após o cadastro da manifestação).

Na busca da melhoria dos serviços prestados, pedimos a gentileza de responder o formulário de avaliação do atendimento, acessando o link:

Formulário de Avaliação

Descrição:
Gostaria de peticionar ao MP para que se inicie um processo do que eu, como cidadão, entendo que deveria ser um Compromisso de Ajustamento da empresa WhatsApp para esta passe a cumprir a lei Lei 12.965/14, especificamente em seu artigo 15.

Esta demanda é baseada em um conjunto de noticias e fatos que demonstram não apenas a razoabilidade e a viabilidade técnica de tal ajustamento, como também que a empresa encontra-se em situação de ilegalidade, tendo optado propositalmente pelo descumprimento da lei mencionada.

Em resumo, os fatos que embasam esta petição são:

1) Decisão recente da Desembargadora Hertha Helena de Oliveira declarando que "Em outras palavras, o Facebook reconheceu que descumpre claramente a obrigação legal que lhe foi imposta pela Lei 12.965/14. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses, nos termos do regulamento", conforme noticiado no dia 21/04/2019 em:

https://www.conjur.com.br/2019-abr-21/facebook-multado-nao-impedir-circulacao-video-whatsapp

2) Relatório (deste autor) demonstrando a viabilidade técnica de rastreamento do remetente inicial de notícias falsas dentro da plataforma WhatsApp através da identificação da URL das mídias (áudio, imagens e vídeos) enviadas.

https://www1.folha.uol.com.br/poder/2019/01/relatorio-enviado-a-pf-sugere-caminho-para-rastrear-fake-news.shtml

3) Resposta oficial do Whatsapp para o Jornal Folha de São Paulo afirmando que não guarda estes registros:

https://www1.folha.uol.com.br/poder/2019/01/whatsapp-nega-ter-registros-que-possam-levar-aos-disseminadores-de-fake-news.shtml

4) Em que pesem algumas imprecisões na decisão da desembargadora Hertha Oliveira por desconhecimento técnico do funcionamento da plataforma, a sua conclusão está essencialmente correta. Em outras palavras é possível demonstrar que:

- O Whatsapp gera um identificador único na forma de URL para cada mídia inserida da plataforma.

- Esta URL é posteriormente utilizada por todos os usuários que receber a mensagem com esta mídia anexada para realizar o "download" da mídia e exibi-la. A URL é também preservada em caso de encaminhamento.

- A URL da mídia pode ser acessada até mesmo em um browser, não sendo possível ao Whatsapp alegar que desconhece a existência desta URL. Não é possível alegar que a URL, em si, seja opaca aos servidores da empresa.

- É também obrigatório, tecnicamente, que o Whatsapp tenha em algum momento feito o mapeamento entre o usuário que enviou a mídia (número do seu telefone) e esta URL. O servidor Whatsapp autorizou que determinado usuário fizesse o "upload" original do conteúdo.

- O Whatsapp possui, sim, a informação de registro do usuário que compartilhou originalmente a mídia. Se a empresa responde que não está guardando este registro para atender a demandas judiciais posteriores ela admite que esta flagrantemente agindo fora da lei.

5) Na opinião deste autor, e também de outros especialistas consultados, o mecanismo de rastreio aqui sugerido oferece uma janela segura para investigações moderadas, isto é, sem permitir abusos e o acesso em massa pelo Estado. Isto se aplicaria também a investigações de diferentes naturezas não eleitorais como, por exemplo, crimes de pedofilia. É necessário avançar com este debate na sociedade, reestabelecendo limites e deveres das empresas de tecnologia para que estas possam colaborar efetivamente com investigações legítimas sem violar os direitos individuais e dentro de suas possibilidades técnicas.

Acrescento na minha manifestação um artigo que escrevi sobre este tema para publicação em revista internacional. O artigo encontra-se em revisão e ainda não foi publicado, porém as informações nele contida podem servir para melhor contextualizar o problema e a demanda aqui colocada.

OBS: Solicitei hoje esta mesma manifestação sob número 20190028020 porém entendo que me equivoquei ao atribuir o município do fato a Niteroi (local originário dos fatos narrados na ação julgada pela desembargadora Hertha de Oliveira) porém sendo a sede da empresa em São Paulo, e sendo também a decisão da desembargadora do TJ/SP, estou abrindo nova manifestação de idêntico teor para ser avaliada no local correto.

É missão do Ministério Público Federal promover a realização da justiça, a bem da sociedade e em defesa do Estado Democrático de Direito.

Atenciosamente,

Sala de Atendimento ao Cidadão - Sistema Cidadão
Ministério Público Federal

FOLHA DE S.PAULO

Relatório enviado à PF sugere caminho para rastrear fake news

Pesquisador coletou dados de 277 grupos de WhatsApp durante as eleições

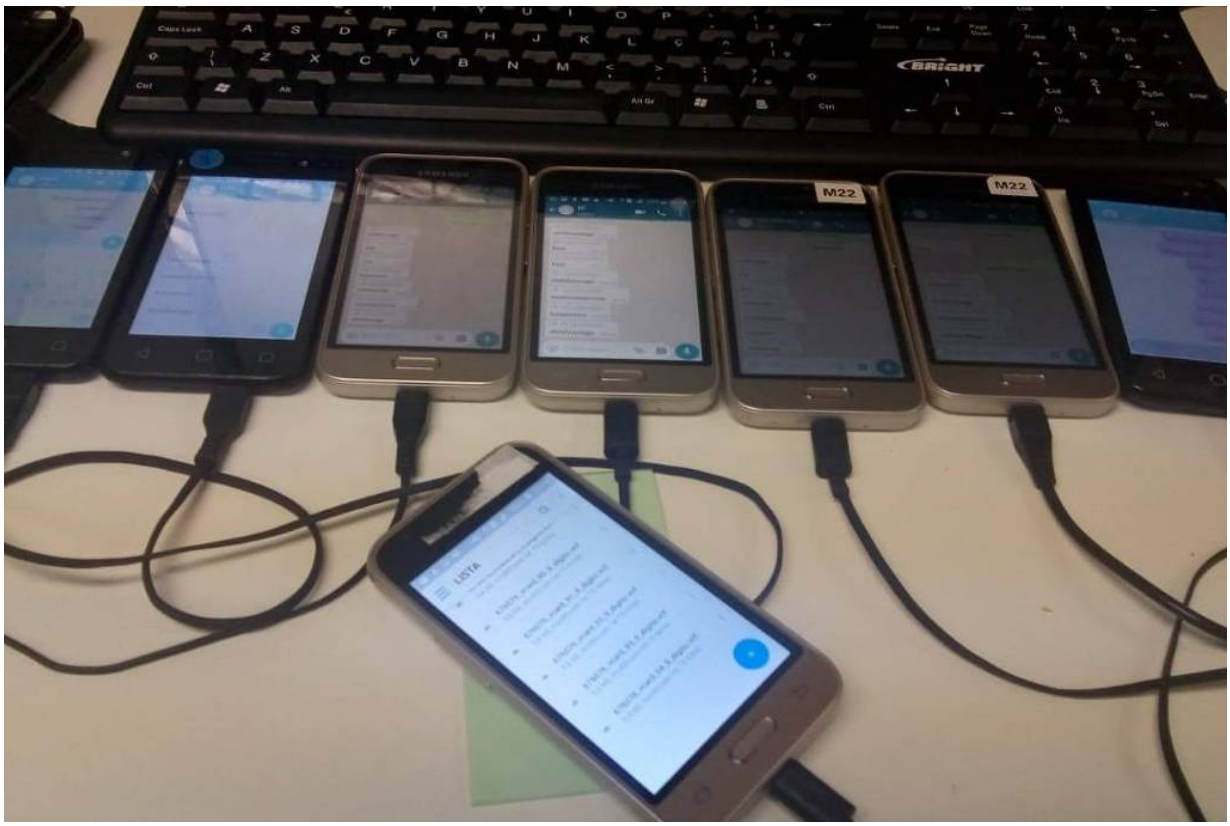
17.jan.2019 às 2h00

EDIÇÃO IMPRESSA (https://www1.folha.uol.com.br/fsp/fac-simile/2019/01/17/)

Patrícia Campos Mello

SÃO PAULO A Procuradoria-Geral da República recebeu, em 26 de novembro de 2018, um parecer técnico com rastreamento de algumas das principais notícias falsas (https://www1.folha.uol.com.br/poder/2018/12/livro-trata-do-dilema-de-como-combater-fake-news-sem-prejudicar-a-democracia.shtml) disseminadas na campanha eleitoral.

O relatório, elaborado pelo especialista em telecomunicações da PUC (Pontifícia Universidade Católica) do Rio Miguel Freitas, permitiria identificar quem foram os primeiros propagadores das mentiras que mais circularam na eleição passada.



Celulares usados em empresa para enviar mensagens de WhatsApp em massa - Reprodução

O documento foi recebido pela procuradora Raquel Branquinho e enviado para a Polícia Federal.

Após negar ter recebido o relatório, a assessoria da PF afirmou que a documentação foi recebida fora dos autos pelo delegado Thiago Marcantonio, responsável por inquérito sobre envio em massa de mensagens pelo WhatsApp nas eleições.

O inquérito foi aberto em 20 de outubro, logo após reportagem da **Folha** mostrar que empresários bancaram envio em massa de mensagens contra o PT (https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml) pelo aplicativo durante a campanha.

Em email a Branquinho, Freitas afirmou que o relatório poderia "auxiliar em algumas linhas de investigação quanto ao uso e disseminação das 'fake news' na eleição de 2018".

Segundo ele, o material reúne "informações técnicas e indícios sobre as origens de algumas das postagens falsas mais relevantes observadas neste processo eleitoral em grupos públicos de WhatsApp".

Freitas diz que sua iniciativa é de caráter pessoal e se colocou à disposição para dar mais esclarecimentos. No entanto, até hoje, quase dois meses depois, ninguém entrou em contato com o pesquisador.

A **Folha** indagou à PF quais medidas haviam sido tomadas a partir do parecer técnico, mas a assessoria limitou-se a dizer que o material foi recebido fora dos autos e não especificou se foi incorporado à investigação eleitoral.

Freitas coletou dados inicialmente de 115 grupos de WhatsApp e posteriormente acrescentou rastreamento de outros 162 grupos, totalizando 277. Identificou 16 notícias falsas de grande circulação na campanha, citadas por órgãos de imprensa.

O relatório chegou a identificadores sobre o primeiro "upload" de cada vídeo ou imagem no WhatsApp.

"Se a Justiça requerer ao WhatsApp os registros que a plataforma mantém em relação a esses identificadores que nós localizamos, será possível chegar ao endereço IP da pessoa que primeiro fez o upload, ou seja, identificá-la", diz ele, coordenador do laboratório de Pesquisa em Tecnologia de Inspeção (CPTI/PUC-Rio).

Segundo o pesquisador, quando um arquivo de mídia é carregado pela primeira vez, ele produz nos servidores do WhatsApp um registro (log) que permite recuperar posteriormente a identificação do usuário que enviou esse conteúdo.

Também é possível conhecer as informações de conexão, como o endereço IP (identificação única de cada computador ou smartphone conectado à rede), a data e a hora.

As mensagens enviadas por um determinado usuário são criptografadas no próprio celular antes de serem enviadas à rede ou aos servidores da plataforma WhatsApp. Esse processo envolve uma chave de segurança que apenas o destinatário possui, e isso garante que nenhum intermediário seja capaz de acessar o conteúdo.

"Esta é a razão da alegação frequente do WhatsApp perante a Justiça de que não seria capaz de fornecer, por motivos técnicos, o conteúdo das mensagens solicitadas", diz.

Os artigos 13 e 15 do Marco Civil da Internet estabelecem obrigações para os provedores de acesso (empresas operadoras de internet) guardar e fornecer por um ano os registros de conexão e, para os provedores de aplicações (caso do WhatsApp), por seis meses.

O parecer do pesquisador chegou a "identificadores" sobre o primeiro upload dessas fake news, que, segundo ele, permitem ao WhatsApp localizar os registros. Não se trata de revelar conteúdo, que não fica nos servidores da plataforma, mas de trabalhar com metadados (dados por trás desse conteúdo).

"É tecnicamente possível obter, via judicial, informações sobre a origem de uma mídia digital enviada ou encaminhada na plataforma WhatsApp. Essas informações incluem o número do celular associado, a hora do acesso e o endereço IP do usuário que realizou o primeiro envio dessa mídia para a plataforma. Mídias digitais, tais como fotos e vídeos, encaminhados entre grupos e entre diferentes usuários dentro da plataforma WhatsApp preservam a capacidade de rastreamento ao usuário de origem", afirma o relatório recebido por Procuradoria e PF.

Segundo Freitas, a solicitação judicial ao WhatsApp deve ser embasada tecnicamente a respeito do funcionamento da plataforma, porque assim se evita que a empresa diga que é inviável atender ao pedido. Como o IP identifica a máquina, seria ainda necessário aprofundar a investigação para encontrar o usuário real.

Nos EUA, o WhatsApp já forneceu esses metadados ao FBI (polícia federal americana) algumas vezes, mediante ordem judicial durante investigação de crimes.

Não é possível dizer se uma pessoa repassou um vídeo ou imagem que veio originalmente do Facebook ou por email.

Mas é possível identificar a primeira pessoa que fez o upload de um conteúdo no WhatsApp. Por mais que não tenha criado o conteúdo, essa pessoa é chave na disseminação —e pode ser um IP de uma agência de marketing ou alguém ligado a algum partido.

ENTENDA AS SUSPEITAS ENVOLVENDO O USO DO WHATSAPP NA ELEIÇÃO

O que está em apuração na Polícia Federal?
Um inquérito foi aberto pela PF após a Folha revelar, no dia 18 de outubro, que empresários impulsionaram disparos por WhatsApp (https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml) contra o PT na campanha eleitoral. As agências que prestavam o serviço eram a Quickmobile, Yacows, Croc Services e SMS Market. A Procuradoria-Geral da República, à época, defendeu a apuração para identificar se a integridade do processo eleitoral tinha sido afetada. A investigação ainda não foi concluída

Quais foram os desdobramentos da reportagem?
No dia seguinte à publicação da reportagem, o WhatsApp, que pertence desde 2014 ao Facebook, bloqueou contas ligadas às quatro agências (https://www1.folha.uol.com.br/poder/2018/10/whatsapp-bloqueia-contas-tse-e-pgr-apuram-atuacao-eleitoral-de-empresas.shtml). Anunciou ainda que baniu centenas de milhares de contas em uma tentativa de conter spam e notícias falsas. Jair Bolsonaro na época negou envolvimento (https://www1.folha.uol.com.br/poder/2018/10/nao-tenho-nada-a-ver-com-isso-diz-

bolsonaro-sobre-empresas-no-whatsapp.shtml) em qualquer irregularidade e disse não ter controle sobre o que empresários apoiadores fazem

Um candidato pode fazer campanha usando o WhatsApp?
Sim, mas as regras previstas em lei precisam ser seguidas. O político pode divulgar propagandas e seus apoiadores podem repassar as mensagens, desde que isso não envolva pagamentos nem sejam usados meios tecnológicos para burlar o sistema do WhatsApp (com o uso deliberado de diferentes chips, por exemplo)

Quem pode receber os conteúdos?
A lei impede que o candidato compre listas de telefones com a intenção de disparar mensagens em massa. O político só pode usar contatos que tenham sido fornecidos pelos donos dos números e que façam parte de base de dados do partido ou do próprio candidato. Empresas estão proibidas pelo Supremo Tribunal Federal de financiar despesas de campanha

O que diz o relatório produzido por Miguel Freitas?
Freitas, especialista em telecomunicações da PUC do Rio, rastreou um total de 277 grupos de WhatsApp e identificou 16 notícias falsas de grande circulação na campanha. O relatório chegou a identificadores que podem apontar a origem de vídeos ou imagens que circularam na eleição

ENDEREÇO DA PÁGINA

https://www1.folha.uol.com.br/poder/2019/01/relatorio-enviado-a-pf-sugere-caminho-para-rastrear-fake-news.shtml

FOLHA DE S.PAULO

WhatsApp nega ter registros que possam levar aos disseminadores de fake news

Segundo a empresa, armazenar esses dados poderia minar a natureza privada do WhatsApp

23.jan.2019 às 15h41

Atualizado: 23.jan.2019 às 22h42

EDIÇÃO IMPRESSA (https://www1.folha.uol.com.br/fsp/fac-simile/2019/01/24/)

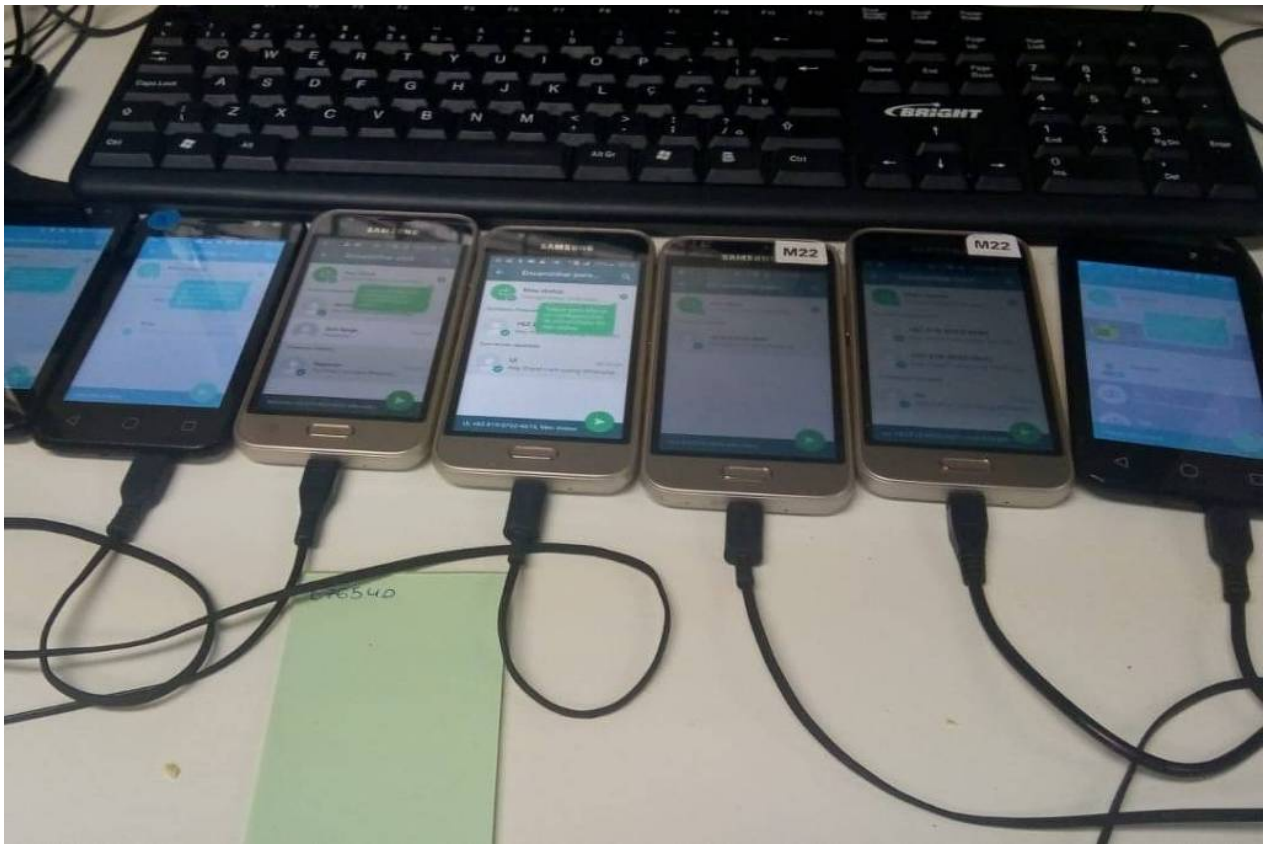
Patrícia Campos Mello

SÃO PAULO O WhatsApp negou que possa fornecer à Justiça os registros referentes a notícias falsas disseminadas durante a campanha eleitoral que permitam encontrar os primeiros disseminadores desse conteúdo.

A nota se refere a reportagem publicada pela **Folha** (https://www1.folha.uol.com.br/poder/2019/01/relatorio-enviado-a-pf-sugere-caminho-para-rastrear-fake-news.shtml)na semana passada segundo a qual a Procuradoria-Geral da República recebeu, em 26 de novembro de 2018, um parecer técnico com rastreamento de algumas das principais notícias falsas (https://www1.folha.uol.com.br/poder/2018/12/livro-trata-do-dilema-de-como-combater-fake-news-sem-prejudicar-a-democracia.shtml) disseminadas na campanha eleitoral.

"Usuários brasileiros enviam milhões de arquivos de mídia no WhatsApp, todos protegidos por criptografia de ponta a ponta", disse a empresa em nota à **Folha**. "Nós não armazenamos dados que identifiquem o primeiro remetente de arquivos de mídia compartilhados no WhatsApp; fazer isso poderia minar a natureza privada do WhatsApp e criar um potencial de uso inadequado", completou.

Um inquérito foi aberto pela PF após a Folha revelar (https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml), no dia 18 de outubro, que empresários impulsionaram disparos por WhatsApp contra o PT na campanha eleitoral. A prática é ilegal, pois se trata de doação de campanha por empresas, vedada pela legislação eleitoral, e não declarada. A Folha apurou à época que cada contrato chegava a R$ 12 milhões.



Celulares usados em empresa para enviar mensagens de WhatsApp em massa durante a eleição - Reprodução

O relatório, elaborado pelo especialista em telecomunicações da PUC do Rio Miguel Freitas, permitiria identificar quais foram os primeiros propagadores das mentiras que mais circularam na eleição passada. O relatório chegou a identificadores sobre o primeiro "upload" de cada vídeo ou imagem no WhatsApp.

"Se a Justiça requerer ao WhatsApp os registros que a plataforma mantém em relação a esses identificadores que nós localizamos será possível chegar ao endereço IP da pessoa que primeiro fez o upload, ou seja, identificá-la", diz Freitas, coordenador do laboratório de Pesquisa em Tecnologia de Inspeção na PUC do Rio.

Segundo o pesquisador, quando um arquivo de mídia é carregado pela primeira vez, ele produz nos servidores do WhatsApp um registro (log) que permite recuperar posteriormente a identificação do usuário que enviou esse conteúdo.

Também é possível, segundo ele, conhecer as informações de conexão, como o endereço IP (identificação única de cada computador ou smartphone conectado à rede), a data e a hora.

As mensagens enviadas por um determinado usuário são criptografadas no próprio celular antes de serem enviadas à rede ou aos servidores da plataforma WhatsApp. Esse processo envolve uma chave de segurança que apenas o destinatário possui, e isso garante que nenhum intermediário seja capaz de acessar o conteúdo.

"Esta é a razão da alegação frequente do WhatsApp perante a Justiça de que não seria capaz de fornecer, por motivos técnicos, o conteúdo das mensagens solicitadas", diz o especialista.

Os artigos 13 e 15 do Marco Civil da Internet estabelecem obrigações para os provedores de acesso (empresas operadoras de internet) guardarem e fornecerem por um ano os registros de conexão e, para os provedores de aplicações (caso do WhatsApp), por seis meses.

O parecer do pesquisador chegou a "identificadores" sobre o primeiro upload dessas fake news, que, segundo ele, permitem ao WhatsApp localizar os registros. Não se trata de revelar conteúdo, que não fica nos servidores da plataforma, mas de trabalhar com metadados (dados por trás desse conteúdo).

"É tecnicamente possível obter, via judicial, informações sobre a origem de uma mídia digital enviada ou encaminhada na plataforma WhatsApp. Essas informações incluem o número do celular associado, a hora do acesso e o endereço IP do usuário que realizou o primeiro envio dessa mídia para a plataforma. Mídias digitais, tais como fotos e vídeos, encaminhadas entre grupos e entre diferentes usuários dentro da plataforma WhatsApp preservam a capacidade de rastreamento ao usuário de origem", afirma o relatório recebido por Procuradoria e Polícia Federal.

Em relação à resposta do WhatsApp, que afirma não manter esses registros, o pesquisador declara que a existência e o armazenamento de dados registrando o acesso e a atividade dos usuários (os chamados metadados ou arquivos de log) são amparados em duas evidências públicas: os Termos de Uso do Serviço WhatsApp, que em seu item 7 fala do armazenamento dos "logs", e uma investigação conduzida pela revista Forbes que analisou o histórico de processos judiciais, encontrando diversos casos em que a empresa de fato forneceu estes metadados para investigações do FBI.

E, caso se negue a fornecer esses dados ou alegue não tê-los armazenado, o WhatsApp estará infringindo o Marco Civil da internet do Brasil.

"Os pesquisadores estão cientes do funcionamento da criptografia ponta a ponta do WhatsApp e, em nenhum momento, colocaram em dúvida sua segurança ou o seu comprometimento com a privacidade do usuário", disse.

Segundo Freitas, pesquisadores demonstraram que, para cada imagem ou vídeo criado pela primeira vez, é gerado um arquivo criptografado que é então armazenado em um servidor web (HTTP) da companhia.

"Ainda que o conteúdo deste arquivo seja protegido por criptografia fim a fim, a existência desta URL, sua criação e seus acessos geram metadados que são de conhecimento da empresa", diz.

"Se o WhatsApp optar por não armazenar estes registros, ele estará possivelmente infringindo o artigo 15 do Marco Civil que exige que provedores de aplicação guardem tais registros pelo prazo de seis meses, sendo obrigados a fornecê-los somente por determinação judicial."

Na última segunda-feira (21), o WhatsApp implementou uma limitação no número de reenvios de conteúdo permitidos pela plataforma (https://www1.folha.uol.com.br/tec/2019/01/whatsapp-limita-reenvios-de-mensagens-a-5-destinatarios.shtml), de 20 para 5 mensagens por vez, para coibir a disseminação de conteúdo viral, como o transmitido durante as eleições.

No entanto, reportagens da **Folha** mostraram que agências de marketing driblam essas limitações (https://www1.folha.uol.com.br/poder/2018/12/fraude-com-cpf-viabiliza-disparo-de-mensagens-de-whatsapp-na-eleicao.shtml) ao usar chips de celular

(https://www1.folha.uol.com.br/poder/2018/12/fraude-com-cpf-viabiliza-disparo-de-mensagens-de-whatsapp-na-eleicao.shtml) de dois chips de celular registrados irregularmente para fazer disparos em massa de mensagem por meio de softwares que emulam a plataforma WhatsApp.

"[O] WhatsApp avaliou com cuidado esse teste [de limite de encaminhamento] e ouviu o feedback dos usuários durante o período de seis meses. O limite de encaminhamento reduziu significantemente o encaminhamento de mensagens no mundo todo", disse a empresa em nota.

"Começando hoje, todos os usuários da última versão do WhatsApp podem encaminhar apenas cinco mensagens por vez, o que vai ajudar a manter o WhatsApp focado em mensagens privadas com contatos próximos. Continuaremos a ouvir o retorno de nossos usuários sobre sua experiência no app, e com o tempo, procuramos novas maneiras de endereçar a questão do conteúdo viral."

ENDEREÇO DA PÁGINA

https://www1.folha.uol.com.br/poder/2019/01/whatsapp-nega-ter-registros-que-possam-levar-aos-disseminadores-de-fake-news.shtml