

1. Identificação da reunião

Data	Horário		Local	Relator
	Início	Término		
16/10/2018	15h00	17h29	Gabinete da Presidência do TSE	Sérgio Três

2. Objetivo

8ª Reunião Ordinária do Conselho Consultivo sobre Internet e Eleições:

Videoconferência com *WhatsApp*, conforme sugerido na reunião anterior, para dirimir questões técnicas pendentes.

Participaram representando a ferramenta *WhatsApp*:

Keyla Maggessy (*Law Enforcement Response and Outreach Manager*)

O Senhor Ben Supple (*Public Policy Manager*)

O Senhor Naveen Pentapelli (*Head of Trust & Safety*)

Advogados: Camila Maruyama e Fernando Neustein

Tradutora:

Danielle Miller (*Portuguese Language Lead*)

3. Participantes

Nome	Lotação
Sérgio Alves	SEPOD/MCTIC
Estêvão André Cardoso Waterloo	TSE - Presidência
Joice Ribeiro Gonçalves da Rocha	TSE – Secretaria-Geral da Presidência
Giuseppe Dutra Janino	TSE - Secretaria de Tecnologia da Informação
Thiago Tavares Nunes de Oliveira	SaferNet Brasil
Maximiliano Salvadori Martinhão	SETEC/MCTIC/CGI
Thiago Fini Kanashiro	TSE - Assessoria de Gestão Eleitoral
Ana Cristina Machado da Rosa	TSE – Assessoria de Comunicação
Humberto Jacques de Medeiros	MPE - Vice-Procurador-Geral Eleitoral
Ciro Leal Martins da Cunha	TSE - Assessoria de Assuntos Internacionais

4. Assuntos tratados

4.1 O Senhor Estêvão André Cardoso Waterloo apresentou-se como Coordenador do Conselho e deu início à reunião, agradecendo a presença de todos e informando que o objetivo principal do encontro é a realização de uma videoconferência com representantes do *WhatsApp* para que as questões técnicas ainda pendentes possam ser discutidas, com vista ao enfrentamento do fenômeno da divulgação de notícias falsas.

4.2 O Senhor Giuseppe Dutra Janino solicitou a participação da empresa que fornece serviços de

segurança junto ao TSE na reunião. Ela trabalha para reduzir a propagação de mensagens de *fake news* e gostaria de saber da possibilidade de implantação de alguma demanda para dar maior celeridade ao TSE nas respostas a serem veiculadas, na forma de API¹.

4.3 A Senhora Keyla Maggessy, representante do *WhatsApp*, autorizou a participação da empresa na reunião.

4.4 Todos os fisicamente presentes no TSE se apresentaram à equipe do *WhatsApp*. A seguir, a palavra foi concedida a eles.

4.5 A Senhora Keyla Maggessy se apresentou, bem como os demais que a acompanhavam: o Senhor Naveen Pentapelli, chefe de segurança do *WhatsApp*, e o gerente de políticas públicas, o Senhor Ben Supple, bem como os advogados Camila Maruyama e Fernando Neustein, assessorando o *WhatsApp*. Por fim, a tradutora se apresentou, a Senhora Danielle Miller.

4.6 A Senhora Keyla Maggessy apresenta que o *WhatsApp* indica que o desafio da desinformação requer ações conjuntas das empresas, sociedade civil e do Governo, e que sua empresa tem se esforçado para colaborar com o Governo, ressaltando que a ferramenta não foi desenvolvida para o mau uso na disseminação de informações inverídicas.

4.7 Na visão da empresa, o combate às notícias inverídicas deve se dar com o foco em três pilares:

4.7.1 buscar a educação dos usuários;

4.7.2 dispor de ferramentas automatizadas para detecção de *spam*² e de análise de contas de usuários com comportamento suspeito;

4.7.3 trabalhar conjuntamente com as autoridades de investigação.

4.8 O primeiro passo é entender como o *WhatsApp* funciona: ele foi desenvolvido para ser uma ferramenta leve, tendo evoluído para hoje dispor de criptografia de ponta a ponta, em quaisquer formatos, seja em mensagens individuais ou de grupos.

4.9 O *WhatsApp* caracteriza-se basicamente pelo envio de mensagens privadas ou em grupos, em média de seis pessoas. No Brasil, esta média é um pouco menor que a média mundial. Sendo assim, não faz parte de sua natureza a divulgação massiva de informações. Seriam necessários quatro mil grupos para se atingir a divulgação de uma mensagem para um milhão de pessoas.

4.10 O *WhatsApp* vem trabalhando com Tribunais Regionais Eleitorais, Partidos Políticos e outros grandes *players*³ em preparação para este processo eleitoral, tendo treinado 1.400 autoridades brasileiras no uso da ferramenta. A Senhora Keyla Maggessy esclarece que participou pessoalmente de pelo menos 12 reuniões, totalizando 600 autoridades, tendo destacado ao público, em especial, como deveria ser formalizado o contato com a empresa para a adequada apuração das denúncias de mau uso do produto.

4.11 Acrescenta que a ferramenta pode ser utilizada por partidos políticos na linha empresarial, por meio do aplicativo *Small and Medium Business* - SMB, com as mesmas políticas de utilização que o *WhatsApp* tradicional.

4.12 O Senhor Ben Supple agradece a oportunidade de poder participar desta reunião, em especial considerando-se o apertado cronograma de todos até a finalização do processo eleitoral.

4.13 Reitera a necessidade de se educar os usuários sobre o uso correto da ferramenta, especialmente considerando-se o tamanho do mercado brasileiro.

¹ Interface de Programação de Aplicações ou Interface de Programação de Aplicação, cujo acrônimo **API** provém do Inglês **Application Programming Interface**, é um conjunto de rotinas e padrões estabelecidos por um *software* para a utilização das suas funcionalidades por aplicativos que não pretendem envolver-se em detalhes da implementação do *software*, mas apenas usar seus serviços, para acesso baseado na *Web*.

² **Spam** é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

³ Os **players** são grupos que dividem sua experiência em um determinado mercado, em uma região específica. Os "grandes *players* do mercado" são as grandes empresas ou pessoas que possuem renome no segmento em que atuam e agem como influenciadores.

4.14 Acrescenta que o *WhatsApp* formou diversas parcerias com a sociedade civil, usuários avançados⁴, empresas de *fact checking*⁵ e mudanças no produto vêm sendo constantemente desenvolvidas para controlar a divulgação das notícias falsas.

4.15 Alerta que o *WhatsApp* vem divulgando campanhas para o adequado uso da ferramenta nos jornais, televisões e revistas.

4.16 Amanhã, 17/10/2018, será lançada uma campanha massiva em 11 cidades brasileiras buscando esclarecer a população sobre as formas de melhor utilização da plataforma. Relata ainda que já ocorreram contratos com 30 empresas de *fact checking*.

4.17 Foi oferecido o *WhatsApp* corporativo para os jornais Estadão e Folha de São Paulo, bem como para empresas de *fact checking*. Este aplicativo corporativo dispõe de mais recursos, para lhes dar maior agilidade de trabalho. Essas entidades verificaram 100 mil rumores que trafegavam na rede do *WhatsApp*.

4.18 Atualmente o *WhatsApp* é o veículo mais rápido de verificação de veracidade de notícias. A empresa está treinando alunos em São Paulo para que se interessem pelo assunto e venham a se tornar *fact checkers*. O objetivo é que possam se tornar propagadores de notícias corretas e identifiquem com maior facilidade as notícias falsas. Esta parceria está sendo expandida com professores para que eles também treinem seus alunos nestas tarefas.

4.19 O produto busca o bloqueio da divulgação viral de informações, principalmente por meio da implementação de alterações no produto:

4.19.1 foram incluídos quatro rótulos nos bancos de dados, os quais facilitam a identificação de mensagens encaminhadas, agilizando o processo de identificação de quem enviou as mensagens. Ou seja, se foi o próprio autor que as enviou ou não;

4.19.2 houve a alteração do limite de envio de mensagens para apenas vinte envios;

4.19.3 foi implementada alteração na rotina de reinclusão de membro a grupo, de modo a dificultar o retorno de um usuário que tenha sido adicionado a um grupo, que tenha solicitado sua exclusão e mudado de ideia posteriormente;

4.19.4 Ainda, a autoridade administradora dos grupos agora pode limitar as conversas nos grupos somente aos administradores.

4.20 Os sinais positivos desta mudança puderam ser observados pela queda em 18% no volume de informações multiplicadas pelo aplicativo após estas alterações terem sido implementadas.

4.21 O Senhor Ben Supple agradece a atenção de todos e coloca-se à disposição para qualquer oportunidade de discussão posterior.

4.22 O Senhor Naveen Pentapelli deseja compartilhar com os demais algumas medidas de segurança que foram implementadas a partir da constatação de comportamentos não adequados: medidas preventivas que ocorrem independentemente da criptografia.

4.23 A tecnologia principal que *WhatsApp* utiliza se dá por uma corrente de envios e denúncias e solicitações de bloqueios. O combate ao *spam* é uma das frentes mais exploradas pelo time de segurança, em especial às mensagens indesejáveis.

4.24 A tentativa, frustrada ou não, de determinado indivíduo tentar obter um número enorme de telefones para envio de informações é observada/controlada pelo *software*, que sinaliza a possibilidade de intervenção.

4.25 O uso de *Machine Learning*⁶ consegue identificar esses sinais e o *WhatsApp* pode fazer o

⁴ Um **usuário avançado** ou um usuário experiente é um usuário de computador que usa recursos avançados de *hardware*, sistemas operacionais, programas ou sites da *Web* que não são usados pelo usuário comum.

⁵ A verificação de fatos ou verificação de dados ou ainda checagem de fatos (também referida pelo termo em inglês **fact-checking**) em jornalismo refere-se ao trabalho de confirmar e comprovar fatos e dados usados em discursos (sobretudo políticos) nos meios de comunicação e outras publicações. Seu propósito é detectar erros, imprecisões e mentiras.

⁶ O aprendizado de máquina (**machine learning**) pode ser entendido como a "habilidade" de computadores aprenderem sozinhos, sem terem sido explicitamente programados. O aprendizado de máquina explora a construção de algoritmos que podem aprender a

banimento destas contas. Sendo assim, informa que o *WhatsApp* bloqueou 700 mil contas antes do período eleitoral. Durante o período eleitoral, também foram banidas contas que apresentavam grande volume de divulgação indevida.

4.26 A parceria com os agentes políticos e partidos deixou claro que o mau uso do *WhatsApp* seria tratado pela empresa.

4.27 O Senhor Naveen Pentapelli encerra sua participação e a Senhora Keyla Maggessy se prepara para apresentar o primeiro vídeo a ser exibido, produzido pelo *WhatsApp*: “Compartilhe fatos, não boatos”. O segundo vídeo exibido trata de um grupo de família na ferramenta e o desvirtuamento de seu objetivo inicial de divulgação de assuntos internos da família por meio da inserção de discussões sobre questões políticas ao longo do tempo.

4.28 O Senhor Humberto Jacques de Medeiros informa à Senhora Keyla Maggessy que o *WhatsApp* vinha sendo tratado como comunicação interpessoal, mas tem surgido uma pressão no TSE para que o *WhatsApp* seja classificado como rede social. Acrescenta que, a partir do primeiro turno das eleições brasileiras, as pessoas buscam uma explicação pelo que as urnas indicaram, especialmente na tomada de decisão do eleitor que utiliza o *WhatsApp*.

4.29 Para as demais plataformas, foram adotados os mesmos três pilares: educação do usuário, *fact checkers* e o direito de resposta. Sendo assim, no dia das eleições, por exemplo, a rede de *WhatsApp* foi tomada por boatos questionando a credibilidade das urnas eletrônicas. Enquanto alguns dos vídeos eram espontâneos, outros haviam sido produzidos com sofisticação, para produzir resultados deletérios.

4.30 Continuando a ser esse o cenário de hoje, não há tempo hábil para se realizar a educação do eleitor e o trabalho de *fact check* é um pouco demorado. No entanto, há o entendimento do MPE de que o *WhatsApp* poderia colaborar com o Brasil.

4.31 O Senhor Ben Supple reitera que o *WhatsApp* não é uma plataforma de mídia social, predominando em seu tráfego as mensagens pessoais, e a média de integrantes por grupo é abaixo de seis pessoas no caso do Brasil. Sendo assim, mesmo que alguns grupos sejam usados por políticos ou partidos, seu volume percentual de envios é bastante reduzido em relação ao uso individual.

4.32 As máquinas de *machine learning* estão sendo usadas para prever este comportamento inadequado da plataforma e tomando providências. Fazendas de *fact checkers* são as equipes mais bem posicionadas para informar sobre a veracidade das informações que circulam na plataforma.

4.33 No exemplo do primeiro turno brasileiro, o Senhor Ben Supple enfatiza que o jornal Globo publicou alguns artigos desmentindo notícias populares que vinham sendo indevidamente multiplicadas por meio do *WhatsApp*.

4.34 Com relação ao direito de resposta, agir com relação a isso dentro do produto do *WhatsApp* agiria contra as políticas de privacidade da ferramenta, bem como de limitações técnicas e da questão inerente à criptografia das mensagens.

4.35 O Senhor Thiago Tavares Nunes de Oliveira se apresenta e coloca suas questões ao Senhor Naveen Pentapelli:

4.35.1 das contas relatadas que foram excluídas por mau uso, quantas foram devido a mensagens de textos e quantas a vídeos?

4.35.2 quantas enviavam para o Brasil e tiveram origem em outros países?

4.35.3 houve a identificação do *WhatsApp* de algum tipo de *microtargeting*?

partir de seus erros e fazer previsões sobre dados. Tais algoritmos operam construindo um modelo a partir de *inputs* amostrais a fim de fazer previsões ou decisões guiadas pelos dados, ao invés de simplesmente seguindo inflexíveis e estáticas instruções pré-programadas.

⁷ **Microtargeting** corresponde à microsegmentação, geralmente usada por partidos políticos e campanhas eleitorais. Inclui técnicas de *datamining* de *marketing* direto que envolvem segmentação preditiva de mercado (também conhecida como análise de cluster). É usada pelos partidos políticos, bem como por candidatos, para rastrear os eleitores individuais e identificar possíveis apoiadores.

As táticas da microsegmentação baseiam-se na transmissão de uma mensagem personalizada para um subgrupo do eleitorado com base em informações exclusivas sobre esse subgrupo. São utilizados vários meios de comunicação, como mala direta,

4.36 O Senhor Naveen Pentapelli relata que irá confirmar se há esta possibilidade de diferenciação de texto/vídeo. Esclarece que o algoritmo de controle de mau uso busca mais a verificação da velocidade de envio das informações que o tipo de informações que estão sendo enviadas.

4.37 O controle do envio dos *spams* não é focado nas vítimas, mas principalmente na fonte do envio, nas contas que disseminam as informações. Outro ponto relevante é que um dos sinais que indicam que uma conta seja um robô é o envio de mensagens para usuários que não fazem parte da agenda do emissor.

4.38 Para finalizar, outra *flag*⁸ para as contas é o envio das mensagens automatizadas com mudança do identificador de país (no Brasil, 55) entre o emissor e o remetente. A identificação não é possível, pois não há a identificação dos usuários do *WhatsApp*.

4.39 O Senhor Thiago Tavares Nunes de Oliveira informa que existem muitos grupos públicos, abertos, destinados à propagação de desinformação, que poderiam ser classificados pelo seu título. Sendo assim, poderia haver uma presunção de que os associados a esses grupos poderiam ser identificados por algum critério por *WhatsApp*.

4.40 O Senhor Naveen Pentapelli informa que esta informação é válida, mas as limitações de criptografia impedem o *WhatsApp* de agir nessas características de foto ou nome do grupo, exclusivamente.

4.41 Acrescenta que a posição da empresa é ser neutra inclusive na interpretação desses sinais, porque não cabe a eles fazer a análise de partidos ou grupos de interesse, baseando suas ações em uma abordagem mais técnica, como a velocidade e ao volume divulgado de mensagens.

4.42 O Senhor Giuseppe Dutra Janino informa que o TSE já aguardava uma onda de *fake news* entre candidatos e partidos, porém a avalanche de ataques foi para a justiça eleitoral, muito bem produzidos e velozmente divulgados. Houve a indicação da existência de uma infraestrutura coordenada para tal fim.

4.43 Acrescenta que o TSE não estava aparelhado para dar as respostas no tempo hábil necessário, em especial para defender a imagem da Justiça Eleitoral. Solicita informar se o *WhatsApp* pode conceder um canal mais célere ao órgão para a produção das respostas.

4.44 A seguir, solicita a criação de uma conta corporativa para dar maior celeridade ao *WhatsApp*.

4.45 O Senhor Ben Supple agradece o questionamento e acrescenta que não há óbice na concessão de uma conta corporativa (*SMB*) ao TSE, o meio mais rápido para oficialmente responder a essas mensagens, e que a plataforma oferece treinamento aos usuários, concedendo inclusive um *checkmark* verde⁹ de autenticidade na conta do TSE, que corresponde a um nível mais alto de autenticidade que o dos próprios *fact checkers*.

4.46 Esclarece algumas questões de infraestrutura para a instalação do programa e explica que o *SMB* pode ser baixado diretamente da respectiva loja (*Android* ou *Apple*) e instalado e configurado em um ou dois dias.

4.47 A opção pelo programa *WhatsApp Business API*, direcionado a negócios de grande porte, demoraria de 6 a 8 semanas para ser implementado dentro da infraestrutura do TSE, e não parece ser o produto mais adequado à demanda manifestada pelo TSE.

4.48 O *WhatsApp* pode fornecer o suporte direto técnico para resolver questões de usabilidade ou defeitos.

4.49 O Senhor Giuseppe Dutra Janino agradece a disponibilidade da empresa e pergunta qual o

telefonemas, visitas domiciliares, televisão, rádio, publicidade na *web*, e-mail e mensagens de texto, entre outros, para se comunicar com os eleitores, criando mensagens para obter apoio para captação de recursos, eventos de campanha e voluntariado.

⁸ *Flag* é uma bandeira, um marcador, um interruptor (ligado/desligado ou ativo/inativo, por exemplo) que permite a otimização de estruturas de dados, na medida em que basta apenas um bit para ativar ou reconhecer determinada característica.

⁹ O *checkmark* corresponde a uma marca de verificação. É uma marca usada para indicar o conceito "sim". 

custo do TSE com a instalação desta conta, bem como do suporte e suas funcionalidades, além do canal de contato para prosseguir com o assunto.

4.50 A Senhora Keyla Maggessy esclarece que o *software* é gratuito.

4.51 O Senhor Naveen Pentapelli esclarece que centenas de milhares de contas foram removidas, mas pode ser que o número de 700 mil não esteja preciso, considerando-se a quantidade de interações entre o tráfego de mensagens dentro do sistema, mas que certamente situa-se na casa das centenas de milhares.

4.52 Prontifica-se em enviar funcionalidades adicionais do *software SMB*, como para a criação de etiquetas de organização de mensagens nos manuais de uso que serão enviadas ao TSE.

4.53 A Senhora Keyla Maggessy agradece a todos a oportunidade e coloca-se à disposição como ponto de contato do *WhatsApp*.

4.54 O Senhor Sérgio Alves pede a palavra e acrescenta que, na política de privacidade do *WhatsApp*, há a indicação de que a empresa informa que, para entregar mídias de maneira mais eficaz, pode haver o armazenamento das informações por mais de 30 dias. Como funcionaria isso dentro do *machine learning* do *WhatsApp*?

4.55 A Senhora Keyla Maggessy reitera que, de fato, todo o conteúdo que trafega pela plataforma é criptografado. Assim, quando uma mídia é carregada pela primeira vez na ferramenta, ela é gravada por meio de uma *hash*¹⁰, que identifica seu conteúdo. No caso deste uso primordial, a *hash* apenas indica qual a mensagem carregada. Assim, se A envia uma mensagem para B, e B a envia para C, não é necessário que B baixe a mídia (*download*) em seu telefone para poder enviá-la a C. Nesse caso, a *hash* inicial é utilizada e a mensagem já é enviada diretamente do servidor.

4.56 Em não havendo sua nova utilização em 14 dias úteis, a mensagem e sua *hash* são excluídas dos servidores do *WhatsApp*. Uma mídia popular só recebe uma *flag* de popular quando sua utilização é grande.

4.57 O Senhor Humberto Jacques de Medeiros pergunta se é possível a identificação da primeira pessoa que subiu uma mensagem.

4.58 A Senhora Keyla Maggessy esclarece novamente que não é possível saber quem fez o *upload* original da mensagem nem a quais pessoas a mensagem foi encaminhada.

4.59 O Senhor Humberto Jacques de Medeiros pergunta como se dá o controle dos vinte encaminhamentos, para controlar a viralização de conteúdos.

4.60 A Senhora Keyla Maggessy esclarece que controlar a quantidade dos envios e controlar quem esteja recebendo os envios são coisas diferentes.

4.61 O Senhor Naveen Pentapelli esclarece que o controle no programa realmente é realizado pela quantidade de *forwards* e não pelo controle das pessoas que estão recebendo as informações.

4.62 O Senhor Ben Supple esclarece que os limites se aplicam individualmente, a cada usuário. Ou seja, cada usuário apenas pode enviar a mesma mensagem para vinte pessoas ou grupos. Os receptores podem multiplicar seus envios a mais vinte pessoas ou grupos, e assim sucessivamente.

4.63 A partir da implementação desta limitação no programa para envio de mensagens a apenas vinte pessoas ou grupos, durante o período eleitoral, observou-se que a redução de envios de mensagens em 18%.

4.64 O Senhor Maximiliano Salvadori Martinhão pergunta se esta regra vale também para os vídeos de *lives*¹¹.

4.65 A Senhora Keyla Maggessy esclarece que o *WhatsApp* não permite *lives*.

4.66 Esclarece que o status do usuário refere-se a uma outra funcionalidade, que pode ou não

¹⁰ **Hash** (escrutínio) é uma sequência de *bits* gerados por um algoritmo de dispersão, que permite o registro inequívoco dele na forma de letras e números, e é utilizado para identificação da mensagem e garantia da integridade dos dados.

¹¹ **Lives** correspondem à transmissão de vídeos ao vivo, no momento em que estão sendo gravados.

ser compartilhada entre as pessoas.

4.67 O Senhor Thiago Tavares Nunes de Oliveira faz a última pergunta, considerando-se a necessidade de liberação da sala que o *WhatsApp* está utilizando para realizar a videoconferência. Seria possível fazer um *scrap*¹² na base de dados olhando apenas os usuários que estejam no Brasil (país 55) e que estejam fazendo parte de milhares de grupos, o que lhes permitiria atingir milhões de pessoas?

4.68 Ou o caminho inverso, onde haja um grupo situado no exterior que seja composto majoritariamente por usuários do Brasil e que pudesse ser identificado.

4.69 O Senhor Ben Supple e o Senhor Naveen Pentapelli esclarecem que esses sinais já são utilizados parcialmente para o controle de *spam* que são utilizados pelo *WhatsApp*. A Senhora Keyla Maggessy informa que irá se informar com os engenheiros se esta extração segmentada seria possível.

4.70 O Senhor Humberto Jacques de Medeiros pergunta novamente sobre a biblioteca de mensagens populares. Seria possível a identificação de quem as recebeu?

4.71 A Senhora Keyla Maggessy reitera que isto não é possível, considerando-se a política de criptografia do *WhatsApp*.

4.72 O Senhor Humberto Jacques de Medeiros acrescenta que gostaria de saber se é possível realizar a transmissão de um serviço de utilidade pública ou de emergência pela ferramenta, como, por exemplo, o envio de uma mensagem para todos os DDDs¹³ de uma região específica.

4.73 O Senhor Ben Supple esclarece que a ferramenta hoje não realiza tal função em nenhuma de suas versões, pois a quantidade de números de usuários continuaria limitada a 20 envios. Implementações de qualquer tipo demorariam de 6 a 8 semanas.

4.74 A Senhora Keyla Maggessy ressalta que esta funcionalidade não está disponível. Ressalta que a utilização da função de *status* teria uma abrangência maior e poderia ser mais bem direcionada para esta funcionalidade.

4.75 Considerando-se a necessidade do *WhatsApp* para liberação de sua sala de videoconferência e a do TSE em iniciar nova reunião com o TRE/RJ, o Senhor Estêvão André Cardoso Waterloo agradeceu a presença de todos, encerrando a sessão.

5. Pendências

5.1 Sem pendências.

6. Anexos

6.1 Foi entregue ao Coordenador do TSE o Ofício n. 91/2018/SaferNet Brasil, com cópia das sugestões para o combate às desinformações (*fake news*) no *WhatsApp*, encaminhadas ao Senhor Ben Supple, Gerente Global de Políticas do *WhatsApp*.

7. Fechamento

Data	Nome do relator
16/10/2018	Sérgio Três

¹² **Scrap** refere-se a uma palavra da língua inglesa cujo significado poder ser *fragmento* ou *pedaço*. Nesse caso, a extração de um segmento filtrado do banco de dados.

¹³ O **DDD** corresponde à sigla de Discagem Direta a Distância, criado para se permitir a realização de ligações interestaduais, considerando-se que cada região do Brasil tem um grupo de prefixos regionais associado às localidades ou cidades.

Tribunal Superior Eleitoral
Secretaria-Geral da Presidência
Documento recebido nesta data:
16/10/2018
Às 12:23
Camilo
Assinatura



Ofício n. 91/2018/SaferNet Brasil
Brasília/DF, 16 de outubro de 2018

À Sua Excelência
Ministra Rosa Weber
Presidente do TSE

Ref: contribuição para o combate a desinformação (fake news) no WhatsApp

Exma. Senhora Ministra

A SaferNet Brasil, associação civil sem fins lucrativos e econômicos, sem qualquer vinculação político-partidária, ideológica ou religiosa, com atuação em todo o território nacional, e levando em consideração as fundadas preocupações objeto de discussões na última reunião do Conselho Consultivo instituído pela Portaria-TSE nº 949, de 7.12.2017, do qual estes signatários têm a honra de serem membros, tem a elevada satisfação em encaminhar a Vossa Excelência, a título de contribuição para os debates no referido Conselho Consultivo, e também como subsídio para a atuação desta egrégia Corte Eleitoral, cópia da manifestação dirigida ao Sr. Ben Supple, Gerente Global de Políticas da empresa WhatsApp Inc.

No documento anexo oferecemos ao WhatsApp um total 8 (oito) sugestões concretas para mitigar os riscos sistêmicos associados a proliferação, em escala jamais vista em outras eleições no Brasil, de desinformação (fake news) fabricada e disseminada deliberadamente com o claro propósito de desestabilizar o processo eleitoral e desacreditar a Justiça Eleitoral perante os eleitores brasileiros.

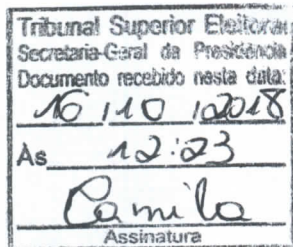
Os subsídios apresentados nesta contribuição são fruto de estudos independentes e levam em consideração os debates travados no Conselho Consultivo do TSE, como também algumas lições apreendidas com a experiência internacional dos signatários no estudo rigoroso da matéria. As sugestões apresentadas são também fruto do diálogo com diversas instituições da sociedade civil interessadas no assunto.

Sem mais para o momento, aproveitamos a oportunidade para renovar nossos votos de elevada estima, respeito e admiração.

Atenciosamente

Thiago Tavares Nunes de Oliveira
Presidente da SaferNet Brasil
Membro Titular do Conselho Consultivo do TSE

Danilo Doneda
Professor Doutor e Consultor do CGI.br
Membro Suplente do Conselho Consultivo do TSE



Brasília/DF, 16 de outubro de 2018

To: Ben Supple
Global Policy Manager
WhatsApp Inc

EXTERNAL POLICY ADVICE

Proposer's brief description:

SaferNet is unique. It's the first-ever NGO in Brazil to established a multistakeholder approach to protect Human Rights in the digital environment. We created and coordinate since 2005 The National Cybercrime Reporting Center, the National Helpline and the Brazilian Digital Safety HUB. We have more than 10 years of experience in delivering capacity building programs with educators, young people, policy makers and law enforcement officials¹ in Brazil.

Since 2014 SaferNet's CEO represent civil society interests at the Brazilian Internet Steering Committee (CGI.br), and served also as a Board Member of the International Hotline Association - INHOPE (based in Netherlands) between 2014 and 2016. SaferNet Brazil has no political, union or religious ties, and has proven technical experience and a long standing positive engagement with the Internet Industry, including Facebook and WhatsApp.

Proposal's motivation:

In December 2017, SaferNet Brazil was formally invited by the Brazilian Superior Court for Elections (TSE) to have a seat at the Advisory Council for Internet and Elections. SaferNet has appointed his founder and CEO, Mr. Thiago Tavares, and Professor Dr. Danilo Doneda, as institutional representatives at TSE's Council.

On that role, we sent on 2nd March, 2018 a formal contribution (annex 1) to TSE with 14 (fourteen) concrete proposals to reduce the impact of misinformation and disinformation during the Brazilian Elections. Those contributions has the focus on 3 pillars: 1) transparency and accountability; 2) economic balance and political ads precification; and 3) media literacy, fact-checking and collaborative journalism.

We are very proud to see that the majority of our proposals was voluntarily accepted and effectively implemented by many stakeholders, including the Tech Giants.

However, in the vacuum of evidence-based research in Brazil on how WhatsApp, which has in Brazil its second major user base in the world, can be used as a political weapon to spread misinformation in a massive scale, we missed the opportunity to predict those trends and fix it before elections started. The effectiveness of spread of information in a

¹ Together with Facebook and WhatsApp, we delivered training sessions for more than one thousand Law Enforcements, Judges and Prosecutors in 11 different cities in Brazil. The positive achievements are public available at: [http:// www.safernet.org.br/workshop-autoridades/](http://www.safernet.org.br/workshop-autoridades/)



massive scale through WhatsApp and its usage combined with techniques specially developed to make possible to disseminate disinformation makes it necessary to consider WhatsApp not merely as a personal communication tool for interpersonal messaging but as a very popular medium to broadcast information - eventually false and misleading.

We consider therefore the relevance of introducing some measures in the platform that, without conflicting with its usefulness and relevance as a very powerful interpersonal communication tool, will be able to make visible and accountable its use as a platform for massive broadcast of information.

Based on our findings and comparative research, we are proposing 8 (eight) policy advices for your consideration. Some of them you are familiar with, and it has been announced by WhatsApp in India, prior to their national elections.

Policy Proposals²

1) Technical measures to be considered to mitigate the risk of WhatsApp (WA) be weaponized to spread misinformation:

- a) WA should consider reducing the number of forwards to five (instead of 20) in Brazil (like was done in India) and by indicating to the receiver whether an incoming message was either forwarded or originally composed by the sender.
- b) WA should consider reducing the number of groups created by a unique user from 9.999 to 499 to avoid automatization behavior. We consider that for the extreme majority of users the limit of 9.999 surpasses by far what would be considered a reasonable volume of groups for personal administration and real interaction, If the user needs to create more than 499 groups, it should be used an specific API or a WA Business Version.
- c) WA should consider defining a reasonable number of group's subscription allowed to a unique user. Nowadays there's no limit, which makes it possible for a unique user to harvest a large amount of data, especially from WA public groups. Again, this limitless possibility doesn't really adds to a better personal experience in communication but it certainly makes it possible to gather large amounts of data - including personal data - on others. If the user want to subscribe a large amount of groups, it should be used the API or WA Business Version.
- d) WA should consider to remove the forward button that appears adjacent to the video or audio message during the elections and campaigning period as a precautionary 'nudge'.

2) Users awareness, fact-checking and evidence-based research:

- a) WA should bring in fact-checking and fake news verification mechanisms to help people check the veracity of content on the platform, through a new feature similar of FB's context tool. The tool should be designed to foster the quality of content and easily provide criteria for the user to better evaluate the material it communicates.
- b) WA should include tools to indicate their users beforehand if any media content they intend to send to groups or multiple recipients is considered to be a piece of disinformation by certified mechanisms. This could be presented as a

² proposals 1a, 1d and 2a was already announced in India: <https://theleaflet.in/wp-content/uploads/2018/08/WhatsApp-fake-news.pdf>



design solution able to create awareness on the controversy on the content before it is posted, as well as a type of flag that would be presented to its recipients, in the case the user decides to send it anyway.

c) WA should work together with TSE, media outlets and civil society to develop new education, awareness and safety materials to improve media literacy and promote civic engagement in app.

d) WA should work with leading academic experts in Brazil to learn more about the spread of misinformation in the country and to produce evidence-based research which can help additional product improvements going forward and better inform policy makers.

These advices aim , above all, to protect the elections' integrity and avoid the app's misuse in Brazil. WhatsApp is a integral part of Brazilians' communication tools and the integrity of its content is a fundamental factor to assure people can continue to trust and use the platform. It's time to look for the future and do our best under the circumstances we face. We hope this policy advice can keep the app core functionals unchanged, and be considerer as a positive contribution for product resilience and improvements during electoral period to enhance safety and combat misinformation.

Yours Sincerely

A handwritten signature in black ink, appearing to read "Thiago Tavares Nunes de Oliveira".

Thiago Tavares Nunes de Oliveira
President of SaferNet Brazil
TSE Advisory Council Member

A handwritten signature in black ink, appearing to read "Porf. Dr. Danilo Doneda".

Porf. Dr. Danilo Doneda
CGI.br Independent Consultant
TSE Advisory Council Member