SENADO FEDERAL
SECRETARIA-GERAL DA MESA
SECRETARIA DE REGISTRO E REDAÇÃO PARLAMENTAR

REUNIÃO
27/11/2019 - 13ª - Comissão Parlamentar Mista de Inquérito - Fake News

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Havendo número regimental e sob a proteção de Deus, declaro aberta a 13ª Reunião da Comissão Parlamentar Mista de Inquérito criada pelo Requerimento do Congresso Nacional nº 11, de 2019, para investigar os ataques cibernéticos que atentam contra a democracia e o debate público, a utilização de perfis falsos para influenciar o resultado das eleições de 2018, a prática de *bullying* sobre o usuários mais vulneráveis da rede de computadores, bem como sobre agentes públicos, e o aliciamento e a orientação de crianças para o cometimento de crimes de ódio e suicídio.

A presente reunião destina-se às oitivas decorrentes dos Requerimentos nºs 90 e 108, de 2019, CPMI *Fake News*, de autoria do Deputado Rui Falcão, do PT de São Paulo, e da Deputada Luizianne Lins, do PT do Ceará.

Estão presentes os seguintes convidados, os quais chamo para compor a Mesa: Sr. Miguel de Andrade Freitas, Sr. Marco Aurélio Rudieger.

Dr. Miguel de Andrade Freitas é Professor da PUC do Rio de Janeiro. Possui graduação em Engenharia pela Pontifícia Universidade Católica do Rio de Janeiro, em 2002, mestrado em Engenharia Elétrica pelo Centro de Estudos em Telecomunicações (Cetuc), em 2004, doutorado em Engenharia Elétrica pela Pontifícia Universidade Católica do Rio, em 2011.

Atualmente, é Engenheiro Pesquisador do Centro de Pesquisas em Tecnologia de Inspeção. Tem experiência nas áreas de engenharia elétrica e ciência de computação com ênfase em redes, telecomunicações, instrumentação e desenvolvimento de *hardware*.

Eu vou passar a palavra - e agradecer a presença antecipadamente - ao Dr. Miguel, para que ele possa contribuir com esta Comissão, pelo prazo inicial de 15 minutos, podendo, evidentemente, se assim desejar, haver uma prorrogação.

Às suas ordens, Dr. Miguel de Andrade Freitas.

O SR. MIGUEL DE ANDRADE FREITAS (Para expor.) - Obrigado, Presidente, Senador Angelo Coronel; Relatora, Deputada Lídice. Obrigado pelo convite para falar nesta Comissão. Eu espero poder contribuir com algumas informações úteis para o trabalho da Comissão.

Eu começo com uma apresentação que é baseada nessa entrega de dois documentos que eu fiz para a PGR, em novembro do ano passado, que foi uma iniciativa de tentar informar as instituições de forma que elas pudessem trabalhar a rastreabilidade do envio de mídias na plataforma WhatsApp para combater crimes digitais.

Então, eu vou passar rapidamente a apresentação, porque teve que ficar em vários eslaides aqui. Ela está organizada nessas duas linhas principais, que foram os dois documentos que eu entreguei, que eu enviei para a PGR, em novembro do ano passado, e eu estou fazendo a entrega formal desses dois documentos aqui. Peço que registrem que eles estão em anexo aqui, no arquivo que eu deixei.

Já me adianto, pedindo um pouco de desculpa aos colegas, aos colegas não, aos caríssimos Senadores e Deputados se a apresentação, eventualmente, ficar com alguns aspectos muito técnicos, mas, justamente, o meu objetivo é trabalhar para corrigir uma assimetria que eu vejo em termos de informação entre o conhecimento da empresa, no caso, do WhatsApp, e o conhecimento que está disponível para os legisladores, para as instituições e para as autoridades. E eu vejo que essa

assimetria de conhecimento a respeito de como essas tecnologias funcionam muitas vezes dificulta que sejam estabelecidas formas de colaboração mais efetivas entre as instituições e essas empresas.

Então, na primeira parte, que corresponde ao documento, eu faço uma demonstração, eu provo, apresentando como funciona o WhatsApp internamente, que é possível a gente fazer um rastreamento da origem de mídias enviadas através da plataforma WhatsApp.

E mídias são arquivos de vídeos, são imagens, são fotos, são áudios e documentos também. Você tem opção no WhatsApp de anexar um PDF, por exemplo. Na segunda parte, eu aplico essa metodologia no caso das *fake news* na eleição de 2018, que foi um trabalho que fiz em conjunto com alguns grupos de pesquisa do Rio de Janeiro que tinham essa base de mensagens que circularam nos grupos de discussão durante as eleições. Aí eu sigo até onde é possível, sem, enfim, uma ordem judicial, que seria uma etapa seguinte desse trabalho.

Pode passar.

Aqui um sumário executivo. A minha apresentação é mostrar que é tecnicamente possível obter, com essa colaboração do WhatsApp, informações sobre a origem de uma mídia digital, que é enviada ou encaminhada através da plataforma. Eu demonstro que o encaminhamento entre grupos e usuários preserva essa capacidade de rastreamento, de forma que a gente possa chegar à primeira pessoa que fez o *upload* da mídia. E destaco uma resposta que o WhatsApp deu, no dia 23/1 - isso foi uma resposta que ele deu à matéria da *Folha*, que cobriu esse trabalho -, de que ele não preservava os registros de *upload* da mídia. Então, eu destaco que essa resposta do WhatsApp pode, possivelmente, constituir uma violação do art. 15 do Marco Civil. Eu vou elaborar um pouco isso mais para frente. E já há uma decisão de segunda instância reconhecendo esse descumprimento. Essa decisão está citada nessa referência que eu coloco aí abaixo, que também está em anexo nos documentos que entreguei.

Pode passar, por favor.

A aplicação da metodologia foi feita nessa base de mensagens de que outros grupos do Rio de Janeiro fizeram a aquisição durante as eleições. Eu fiz análise de 16 casos específicos, quer dizer, 16 mensagens de conteúdo falso, por critérios de relevância e de melhor rastreabilidade. Todo esse material foi entregue, foi encaminhado para a PGR por *e-mail*, em 26/11/2018, como uma contribuição pessoal a essa investigação. O que eu tinha de informação de imprensa era que se tratava de uma investigação que estava em andamento a pedido da PGR. Então, eu fiz esse envio justamente para a PGR. E destaco que é uma contribuição pessoal. Isso não tem relação com o meu trabalho de pesquisa direto na faculdade. E eu também não sou filiado a nenhum partido, a nenhuma empresa em relação a essa contribuição.

Pode passar.

Aqui eu começo a entrar um pouco na parte técnica do funcionamento do WhatsApp. Eu fiz alguns diagramas aqui. Eu só queria destacar o conceito-chave dessa tecnologia que a gente chama de criptografia fim-a-fim, porque, na verdade, historicamente, isso é uma questão inédita. Você tem um empoderamento do usuário onde ele é capaz de garantir a privacidade, a própria privacidade com recursos que ele tem no seu celular. Então, se você for olhar num período histórico, a gente sempre teve os indivíduos dependendo de garantias das instituições para preservar a sua privacidade, e agora você tem um empoderamento: o próprio aplicativo que roda no seu celular criptografa a sua mensagem. Aqui, neste exemplo, digamos que você tem esse "Bom dia!" enviado do celular da esquerda para o da direita. Digamos que o João mandou um "bom dia" para a Maria.

Essa mensagem "bom dia", no momento em que sai do celular do João, está codificada, criptografada, está representada por aquele conjunto de zeros e uns ali, e, de fato, ninguém fora do celular do João ou da Maria sabe o conteúdo dessa mensagem. E aí há toda uma discussão, que é bastante interessante, do que o WhatsApp pode efetivamente fornecer em termos de informação dessa troca de mensagem, que é a questão dos dados *versus* os metadados. Então, o servidor do WhatsApp sabe que uma mensagem foi enviada do João para a Maria, mas ele não sabe o conteúdo dessa mensagem. Sempre que essa discussão vem à tona do WhatsApp, "mas o WhatsApp não tem como burlar", realmente não tem como burlar. Então, tecnicamente, de toda a informação que a gente tem de como o sistema funciona, ele é bastante seguro.

E aqui eu destaco como funciona o envio de mídias, que, na verdade, segue por um caminho um pouco diferente do caminho da mensagem em si. Eu destaquei ali, ele segue por dois caminhos: um caminho verde para as mídias e um caminho vermelho para as mensagens.

Então, digamos que, nesse exemplo aqui, novamente o João está querendo mandar a foto da Monalisa para a Maria, e junto daquela mensagem verdinha, que poderia ter o "bom dia", ele quer mandar essa imagem. O que acontece no processo aqui é que a mensagem é criptografada separadamente primeiro, isso gera um arquivo criptografado, que está representado com aquele cadeado verde ali, esse arquivo é enviado para os servidores do WhatsApp e fica disponível em um servidor *web* -

do WhatsApp ou do Facebook - da empresa que hospeda esses arquivos, e dois campos estão inseridos na mensagem texto em campos escondidos, que são a URL e a chave. A URL é aquele endereço que a gente coloca... A gente pode pegar essa URL e colocá-la no Browser, aí a gente vai conseguir fazer o *download* deste arquivo. Só que se eu faço o *download* de um arquivo criptografado, eu não consigo entender o conteúdo dele, eu só consigo entender o conteúdo dele se eu tiver a chave, que é como se fosse uma senha para converter novamente aquele arquivo, que é aquele cadeado verdinho, para a imagem da Monalisa. Então, o ponto aqui é que esse caminho de envio de um arquivo de uma mídia é um pouco diferente do caminho normal de envio de uma mensagem puramente de texto. E aí por que eu estou destacando isso?

Pode passar, por favor.

Aqui é um experimento simples - que qualquer usuário de WhatsApp pode fazer - de usabilidade. Ele pode perceber a diferença que tem quando ele faz um *upload* - ele gravou um vídeo e está fazendo um *upload* desse vídeo - e ele observa aquele círculo de progresso na interface do WhatsApp. Se, por outro lado, ele está fazendo um repasse, um encaminhamento de uma mensagem, geralmente esse encaminhamento é instantâneo, não há um indicador de progresso e o tique de que a mensagem foi enviada aparece imediatamente.

Passe, por favor.

Aqui é a explicação de por que isso acontece. Quando você faz esse encaminhamento, digamos que a Maria agora está encaminhando aquela mensagem que ela recebeu com a imagem da Monalisa para uma outra pessoa, ela encaminha apenas as referências que permitem recuperar a mensagem, ou seja, ela encaminha apenas as informações que são a URL de onde o arquivo criptografado está hospedado, que é aquele arquivo verdinho com cadeado lá em cima, e a chave, que seria a senha criptográfica para você poder recuperar o arquivo original, mas a diferença é que não há um novo *upload* desse arquivo.

Nesse eslaide, essa lupa representa um detalhe passo a passo de como é que esse processo é feito. Eu não vou seguir esse passo a passo. Deixo aqui só como referência na apresentação, porque isso aqui é para provar o meu ponto no próximo eslaide.

Bom, então aqui é uma comparação que eu faço entre aplicações, à luz do que a Lei do Marco Civil da Internet diz. E você tem, na coluna ali do meio, a comparação com as aplicações tradicionais, porque a Justiça hoje já está habituada cotidianamente a dar ordens judiciais para obter informações sobre quem foi o autor daquele conteúdo. E eu comparo isso com o que acontece com o WhatsApp.

Então vocês podem ver que nos dois casos, basicamente acontece o mesmo processo. As duas aplicações, tanto, por exemplo, uma página de Facebook, você não sobe uma página de Facebook se você não estiver logado na sua conta de Facebook; da mesma forma, você não faz um *upload* no WhatsApp se você não estiver logado na rede do WhatsApp. Então a autenticação é exigida. O servidor que recebe aquele *upload* conhece o endereço IP do terminal que está fazendo o *upload.* Nos dois casos, é gerada uma URL, que é um identificador inequívoco, nos termos da Lei do Marco Civil, art. 19, §10.

E o que a gente está acostumado a ver é que as hospedagens de *site*, as páginas dessas aplicações tradicionais, provedores de aplicação conhecidos são obrigados a manter os registros de acesso por seis meses. Isso é o que diz o art. 15. E no caso do WhatsApp, essa questão me parece que nunca foi colocada; mas eu não vejo nenhum motivo técnico pelo qual o WhatsApp seria desobrigado de cumprir com esse mesmo artigo.

Pode passar, por favor.

Aqui a gente já entra na parte da aplicação nas eleições. Então essa é uma imagem que foi elaborada pelo grupo da UERJ. A referência está ali embaixo. O artigo também está em anexo. A gente pode ver como é que uma notícia falsa se propaga, viraliza entre os grupos. Aqueles pontinhos ali seriam grupos de discussão política, e as linhas são usuários que participam de mais de um grupo, e eles fazem a ponte, fazendo o repasse entre os grupos, produzindo esse processo de viralização. Então a gente percebe que começa ali às 11h da manhã, e à medida que o dia passa, você vai aumentando o alcance dessa propagação dessa notícia, que no caso era uma notícia falsa, por esse processo.

E fazendo uma amostragem, e aí amostragem significa participar desses grupos de política, que, muitas vezes, têm convites públicos disponibilizados e trocados em diversos meios, você consegue uma amostragem de como está funcionando essa dinâmica de propagação de *fake news.* Não quer dizer que você vá ter acesso a todas as...

(Soa a campainha.)

O SR. MIGUEL DE ANDRADE FREITAS - ... propagações, não é? Essa estimativa ali de alcançados são apenas dos grupos que foram amostrados, mas a dinâmica que você analisa nessa escala é a mesma dinâmica na escala global de toda a rede.

Então, aqui foram analisados os dados de 277 grupos de política no período eleitoral e pré-eleitoral, que tinham convites públicos. Isso é para todos os candidatos da eleição. Uma base de 799 mil mensagens, 15 mil participantes e 120 mil imagens compartilhadas.

Pode passar.

Só que, para fazer uma análise de propagação de mensagens específicas, a gente tem que ter um critério para selecionar essas mensagens. Então, o primeiro critério que eu adotei foi pegar uma seleção que foi feita pelo jornal El País, que é uma matéria chamada "Os 'whatsapps' de uma campanha envenenada", que é uma matéria bastante interessante, porque ela mostra o que era um tráfego típico de mensagens compartilhadas nessas mídias, então eu peguei... eu localizei essas imagens nos grupos e fiz análise de rastreamento desses casos.

E os outros critérios seriam as imagens mais compartilhadas e que fossem comprovadamente falsas por *sites* de verificação de informações; e essas mídias falsas que tinham as melhores características de rastreamento. E aí é um critério importante, que se trata de a URL, de a mídia ser preservada entre os encaminhamentos. Quando isso não acontece, é um indício de que a mensagem se propagou provavelmente por um outro meio, talvez uma outra plataforma de rede social, antes de ser colocada no WhatsApp.

Eu vou dar um outro exemplo, acho que é no próximo eslaide.

Então, justamente, essa aqui é a seleção da matéria do El País, e o que aconteceu foi que, embora todas essas imagens, eu tenha feito a análise de propagação delas nos grupos, em alguns casos essa rastreabilidade não era boa, porque a URL não se mantinha,...

(Soa a campainha.)

O SR. MIGUEL DE ANDRADE FREITAS - ... ela não se preservava ao longo da propagação da mensagem nesses grupos. Mas, de qualquer forma, essas informações estão no relatório, que eu anexei e entreguei na PGR.

E aqui eu tenho já um exemplo oposto, que é um exemplo de uma excelente rastreabilidade, eu diria até mais do que boa, que é... a imagem está ali no canto, é difícil de ver, porque ela está muito pequena, mas é uma suposta conversa entre o Fernando Haddad e o Sergio Gabrielli, combinando que eles fariam uma matéria *fake* na *Folha de S.Paulo*, e essa matéria *fake* supostamente seria a matéria sobre o envio massivo de mensagens pagas com caixa dois, enfim foi aquela matéria que deu toda aquela repercussão, então essa imagem seria o candidato...

(Soa a campainha.)

O SR. MIGUEL DE ANDRADE FREITAS - ... combinando forjar uma matéria na *Folha*.

E aí, ali embaixo, é um exemplo da listagem onde você tem o horário em que a mensagem foi vista em cada grupo, e o que a gente pode perceber é que a URL encontrada em todos os grupos é a mesma. Então, isso indica que todas essas ocorrências da mensagem são encaminhamentos sucessivos de um único *upload* original, que poderia então ser usado para um processo de investigação.

Pode passar.

O caminho para continuar essa investigação a partir desse relatório seria solicitar, por ordem judicial, ao WhatsApp os registros de acesso do usuário responsável pelo *upload* desse arquivo, que se encontra hospedado nessa URL - é uma URL dentro dos servidores do WhatsApp. Eu, por curiosidade, ontem de noite, cliquei de novo nesse *link*, esse arquivo continua lá; quer dizer, se você clica nesse *link*, você baixa um arquivo de 70k, que é aquela imagem; você não vai ver essa imagem, eu preciso te dar também a senha, para você descriptografar e ver aquela imagem específica, mas esse arquivo continua no ar, ou seja, se alguém daquela lista fizer um novo repasse, vai continuar preservando essa mesma URL, que foi criada pelo primeiro usuário da plataforma WhatsApp e fez o *upload* desse arquivo.

Então, pode passar também.

Considerações finais sobre o trabalho. Foram analisados, então, 16 casos de *fake news* que circularam em grupos de política, extraindo essas URL, que poderiam servir para elaborar solicitações judiciais. Aqui é uma especulação minha de que seria improvável que o WhatsApp ainda possua esses registros da época, ainda mais considerando que eles deram uma resposta no início do ano dizendo que eles não guardavam esses registros, que é justamente essa discussão quanto ao WhatsApp estar infringindo um artigo do marco civil. Acredito que um ajustamento de conduta da empresa nesses termos permitiria investigações nessa forma que eu estou descrevendo.

Tem só mais um.

E, na minha opinião, esse mecanismo de rastreio que eu estou propondo aqui sugere uma janela segura para investigações moderadas, sem abusos e acesso em massa pelo Estado. Naquele momento em que eu disse que há um empoderamento do usuário com a possibilidade de garantir a sua própria privacidade hoje, eu entendo isso como um movimento que visou combater um acesso em massa pelo Estado. A gente teve aquele caso do vazamento do Snowden, onde, quando as informações não eram criptografadas fim a fim, você poderia com muita facilidade tecnológica monitorar as conversas privadas de todo mundo. Então, essa criptografia do WhatsApp, do Telegram e de todos esses aplicativos vem como uma resposta de certa forma a essa questão, mas acredito que a gente pode avançar com esse debate.

Talvez os trabalhos da CPMI possam sugerir uma colaboração maior com as empresas para que, dentro dos limites tecnológicos que essas empresas operam, elas possam colaborar efetivamente com investigações previstas em lei, como, por exemplo, a lei de interceptações telefônicas que a gente tem, que é uma lei que é muito clara nos casos que isso pode ocorrer, não seria uma invasão indiscriminada da privacidade das pessoas.

Então, é essa a minha apresentação e fico aqui disponível para esclarecimentos e perguntas.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Obrigado, Dr. Miguel.

Então, vamos ouvir agora o Marco Aurélio e, depois, vamos para a sessão dos debates.

O SR. MARCO AURÉLIO RUEDIGER (Para expor.) - Boa tarde a todos.

Eu sou Diretor de Análise de Políticas Públicas da Fundação Getúlio Vargas, doutor em Sociologia Política, mas eu queria deixar claro, desde o início aqui, que o que eu vou apresentar aqui, as opiniões aqui são de minha inteira responsabilidade e não representam a posição oficial da Fundação Getúlio Vargas, a instituição que eu trabalho, em absoluto. Então, é uma contribuição, digamos assim, em temos cívicos, que pretendo dar, e em termos pessoais. Com ajuda de alguns colegas, elaboramos aí essa pequena apresentação. O objetivo é que ela seja muito rápida e muito sucinta, mas que ela dê espaço para a gente poder fazer depois um debate mais substantivo.

A questão que eu queria trazer para vocês, eu queria começar por um ângulo da Sociologia Política, em si, para dizer que o fenômeno que a gente está enfrentando não é um fenômeno que ocorre a partir das eleições do ano passado. A gente já identifica, no nosso laboratório, a presença de processos de desinformação organizada desde antes de 2014. Vou mostrar alguns exemplos a vocês daqui a pouco, mas desde antes de 2014 a gente vê esse processo ocorrendo. Ele vem se intensificando de forma bastante significativa. Isso, no meu entender, joga uma sombra extremamente preocupante em relação às instituições do País e ao próprio processo democrático. Queria ressaltar isso para vocês, deixar bem claro em termos de uma condição basilar do que vou falar daqui para frente. No final, vou trazer para um campo muito concreto e propositivo.

Adiante, por favor.

Isso daqui, é para a gente olhar em termos gerais, esquemáticos, o que seria desinformação. Desinformação, eu diria a vocês, é termo que se usa hoje, correntemente, na área. A gente tem parceria com o Atlantic Council, com o National Democratic Institute e com outras instituições de pesquisa. Basicamente, a preocupação geral não é só com *fake news*, mas com o processo de desinformação num sentindo muito mais amplo, que não é feito só por uma notícia maliciosa e deturpada, mas, sim, por todo um processo de convencimento em massa de percepções, com base, muitas vezes, até em verdades, mas que visam a distorcer e a quebrar a credibilidade no próprio processo político, nas instituições.

Por favor.

Então, em geral, na produção... Um conteúdo anônimo é bastante percebido. Quando eu digo que é anônimo, às vezes, existe uma foto, existe um nome, mas não é de fato uma pessoa. Isso aí tem uma conjugação muito forte com um processo de polarização que a gente tem atravessado no País.

Num segundo momento, a disseminação se dá através de redes de automação, que são ecossistemas de automação, na verdade. Quando eu falo rede, eu não falo só de uma plataforma, mas de uma estrutura sistêmica de vinculação de várias plataformas. Esse é o ponto muito importante. Há um disparo em massa, que é um outro ponto importante. Finalmente, isso é complementado por influenciadores e comunidades de influenciadores que operam de forma aderente às estruturas de desinformação automatizadas. Então, a gente está falando aqui de um sistema inteiro de composição. E o impacto disso qual é? Uma distorção brutal da informação, que já é simétrica e se torna muito mais; um processo de difamação e de destruição de reputações consistentes sustentado, planejado e, finalmente, a quebra de confiança nas instituições.

A quebra de confiança nas instituições, a meu ver, é o aspecto mais nocivo e pérfido desse processo porque, no momento em que não existe confiança, não existe contrato. O que precede um contrato é a confiança. Então, quando se quebra a confiança se trafega no niilismo absoluto em relação às instituições e aos pactos sociais.

Daí, abre-se espaço para qualquer tipo de aventura ou de proposta que seja antagônica à própria democracia. Isso eu acho que é extremamente danoso e, por isso, eu digo que nós vivemos um momento extremamente complexo que exige de todo o aparato institucional, estatal e cívico uma atenção extremamente grande, principalmente porque se avizinham eleições agora.

Em frente, por favor.

Então, só como um resumo. A automação com o uso anônimo e disseminado de redes de robôs, mas não só de robôs, o.k., para atacar adversários, espalhar notícias falsas e atingir de forma intencional valores e regras democráticas. Esse é o ponto central!

Em frente.

As características seriam uma automação... Mas eu quero lembrar vocês que anteriormente eu falei que influenciadores fazem parte do processo também, não só perfis automatizados, mas os perfis automatizados têm um propósito, o espalhamento de ampliação da capilaridade em tempo real numa compressão do tempo numa rede de progressão e impactos bastante acentuados. Basicamente, só para fazer uma síntese, *posts* com menos de um segundo, utilização de plataformas, o que aqui eu quero dizer que são *softwares* ou fazendas com administração de contas, aqui ou no exterior. Isso é importante entender, que do exterior também há muita desinformação do que ocorre no Brasil e os trabalhos nossos, da minha unidade que lidero na fundação, já foram publicados aqui e também no exterior, são de conhecimento no exterior de várias organizações, até o Departamento de Estado dos Estados Unidos tem cópias desses trabalhos.

Disseminação em massa também é outro ponto importante.

Vamos em frente.

Isso aqui é uma tipologia de robôs, eu não vou me alongar aqui. Só queria ressaltar que nem todos os robôs são maléficos, nem todos os robôs são nocivos, nem todos os robôs são ilegais, há robôs, por exemplo, de organizações, de bancos, que ajudam no nosso dia a dia. Então, é muito importante ter essa distinção.

Então, o que caracteriza os robôs que são maliciosos? É isso que me interessa, é isso que a gente está olhando, é disso que se trata aqui.

Em frente.

Aqui, finalmente, eu mostro para vocês o que é uma onda de disseminação a partir de um robô. Então, o que está ali em rosa são perfis automatizados, o que está em azul são perfis humanos e cada uma dessas linhas que nós vemos aqui, e que eu ali embaixo chamo de grau 1, 2, 3 e 4, é a distância entre uma pessoa e a seguinte dentro de uma rede. A gente vê que a partir de um perfil totalmente automatizado, e esse é identificado como um potencial mecanismo, um algoritmo, que, em outras palavras, eu poderia chamar de robô, influencia não só pessoas de forma orgânica, mas, também, repassa para outros robôs essa informação. Uma vez repassada essa informação, ela vai para o nível 2, pessoas que receberam essa informação e acham que, de alguma forma, tem alguma validade, repassam adiante e assim sucessivamente numa onda de impacto.

Nesse caso específico, eu estou pegando um caso específico, num dia específico. Eu trato no laboratório com milhares de casos por dia, filtrados por dicionários linguísticos gigantescos, que são criados por nós, numa metodologia extremamente robusta e conservadora até, eu diria, no sentido de identificar o que é e o que não é. A gente tem um cuidado muito grande de não cometer erros. Os nossos bancos de dados, inclusive, já passaram por outras instituições que olharam e a gente faz esse tipo de averiguação.

Basicamente, a partir de uma informação que foi automatizada, o impacto ali, esse especificamente atingiu usuários únicos, 1.521, sendo 250 robôs. Em vários casos desses, um outro robô replicou para outros robôs.

Então, o que a gente está falando aqui...

A SRA. KÁTIA ABREU (PDT - TO) - Pela ordem, Sr. Presidente. Sr. Presidente, pela ordem. Posso tirar apenas uma dúvida aqui?

O SR. MARCO AURÉLIO RUEDIGER - Sim.

A SRA. KÁTIA ABREU (PDT - TO. Para interpelar.) - O robô pode ser implementado num pré-pago ou só no pós-pago? No telefone, no *chip*.

O SR. MARCO AURÉLIO RUEDIGER - Aqui eu não estou falando de WhatsApp, eu estou falando de Twitter especificamente, tá?

A SRA. KÁTIA ABREU (PDT - TO) - O.k.

O SR. MARCO AURÉLIO RUEDIGER - Mas, para responder essa sua pergunta de uma forma muito sintética, no WhatsApp os envios podem ser automatizados também.

A SRA. KÁTIA ABREU (PDT - TO) - No pré-pago? No pós-pago?

O SR. MARCO AURÉLIO RUEDIGER - No pós-pago. No pré-pago, eu não tenho certeza... Nos dois, com certeza. Os dois, então.

Bom, isso aqui é para dar uma dimensão com o que a gente está lidando. É um negócio que eu acho importante, porque são em milhares. Eu não estou falando de um, estou falando de milhares.

Vamos adiante, por favor.

Então, aqui, em 2014, já na eleição. A gente viu na eleição de 2014 a polarização, utilização em vários campos de robôs. Eu diria para vocês que a utilização de robôs não é privilégio num campo, eu não estou endereçando isso a um candidato específico, eu estou falando de campos. O.k.? Não é, muito embora haja campos que utilizem de forma muito mais significativa e muito mais eficaz do que outros.

Vamos adiante.

Essa aqui já foi na eleição de 2018. Se não me engano, foi no primeiro turno. Em setembro, no primeiro turno.

A gente tem... Aqui a gente fez uma um mergulho um pouco mais profundo, até porque no segundo turno fica mais fácil ver os polos, não é isso? Então, no primeiro, a gente tem o centro, o centro político ali. O campo rosa e o campo laranja são muito mais fracos na utilização de qualquer tipo de mecanismo desse tipo. As polaridades usam muito mais. E eu estou falando de novo de campos, eu não estou endereçando isso a nenhum candidato, quero que fique claro isso. Mas isso é um fato. Isso é um fato comprovado numericamente e estatisticamente. Esses bancos de dados podem ser abertos para qualquer um tirar qualquer dúvida.

Vamos em frente, por favor.

E no final a gente tem um processo de polarização que é extremamente acentuado pela avalanche de informações que concorrem em tempo real, 7 por 24 - sete dias da semana, 24 horas por dia -, radicalizando e polarizando o processo.

Vamos em frente.

Aqui... E esse é um ponto muito importante. Essa situação hoje dos perfis que existem atuando nas discussões nas redes. E nesses perfis eu acho que eu não incluí aqui os robôs, mas há robôs funcionando no debate hoje. Ou seja, há um contínuo que não se limita somente às eleições.

Então, o processo político todo hoje, o processo do debate e o processo de auscultar a sociedade civil através de redes sociais...

A SRA. NATÁLIA BONAVIDES (PT - RN) - Licença, Presidente.

O SR. MARCO AURÉLIO RUEDIGER - ... ele é influenciado pelo debate orgânico, mas também tem um debate no orgânico subjacente a ele que opera e distorce por vezes.

A SRA. NATÁLIA BONAVIDES (PT - RN) - Para tirar uma dúvida.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Dr. Marco, questão de ordem dali, da Deputada, para esclarecer.

A SRA. NATÁLIA BONAVIDES (PT - RN) - Obrigada, Presidente.

O SR. MARCO AURÉLIO RUEDIGER - Desculpa.

A SRA. NATÁLIA BONAVIDES (PT - RN. Para interpelar.) - Esse eslaide, então, é sobre perfis do Twitter? Não é sobre robôs, é sobre influência de perfis individuais?

O SR. MARCO AURÉLIO RUEDIGER - Esse aqui é perfil de Twitter, mas eu poderia tranquilamente botar os robôs aqui, acho que a gente simplesmente não colocou...

A SRA. NATÁLIA BONAVIDES (PT - RN) - E aí o tamanho do nome do perfil equivale ao tanto...

O SR. MARCO AURÉLIO RUEDIGER - O perfil é o tamanho na rede. Exatamente.

Evidentemente a polarização é muito grande, principalmente entre alguns segmentos de esquerda e de direita mais extremos. Isso é tranquilo.

Vamos adiante.

Então, disparo em massa, eu falei já de fábricas. Não vou demorar nesse eslaide.

Passe adianta por favor.

Aqui é a ideia do ecossistema. É importante isso, porque por exemplo o WhatsApp, como disse o professor que me antecedeu, o WhatsApp tem grupos públicos; ele puxa as pessoas através de grupos públicos para uma série de debates, depois as pessoas são convidadas para outros subgrupos, para outros subgrupos, que, a partir dali, uma série de materiais de divulgação são repassados e depois eles transbordam para as plataformas mais tradicionais de debates. Não só as plataformas tradicionais operam, mas...

(Soa a campainha.)

O SR. MARCO AURÉLIO RUEDIGER - ... outras plataformas também têm vínculos com isso. O reddit tem, por exemplo, a ver com isso. Ali o GAB, o sapo verde, por exemplo, é uma rede especificamente de extrema direita e que tem uma presença, assim, de brasileiros quando se olha a fundo essa rede. E dali sai muita informação, muita desinformação que alimenta também esse complexo todo. O sapo ali, o GAB. E outras redes, enfim, TikTok, Instagram. Então, a gente está falando de um complexo. É muito mais sofisticado do que simplesmente a gente pensar numa plataforma só.

Vamos em frente.

Então, a circulação nas redes sociais, eu vou tentar ser um pouco mais objetivo, que o WhatsApp já foi abordado interiormente aqui. O WhatsApp tem o compartilhamento de conteúdo que se espalha depois, permeia as outras redes, que pode ser legítimo ou ilegítimo - esse é o ponto.

Vamos em frente.

Redes de influenciadores. Esses, digamos assim, é um problema que eu acho bastante sério.

Vamos em frente.

Eu vou mostrar... Isso aí é uma rede de influenciadores dentro do YouTube. Então, a gente fala muito aqui do WhatsApp, a gente fala muito do Facebook, a gente fala do Twitter... Eu queria até fazer uma ressalva: eu acho que o Twitter é uma das redes mais *accountable* que há, mais aberta. Já o Facebook é o contrário; é uma rede que historicamente tem-se fechado cada vez mais em termos da sua parte pública para observação dos analistas, dos pesquisadores. Não acho que seja à toa que no congresso americano o Mark Zuckerberg tenha sido chamado constantemente, questionado sobre as práticas da organização dele nesses termos.

Mas se a gente olhar o YouTube, por exemplo, nele há uma presença extremamente complexa, crescente e eu diria em termos de informação importante, mas também muito perigosa em certo aspecto. Por exemplo, um debate que começa 10h e termina meia-noite. O.k. Perfeito, muita gente não vê. No outro dia as pessoas vão ao YouTube para ver o quê? Ver a edição do debate; vão ver uma versão específica. É uma outra narrativa; é uma pós-verdade em relação ao fato, à verdade que foi o debate. Cada um pode fazer sua propaganda do jeito que quiser.

O problema todo é quando chegam influenciadores que não se sabe quem dirige, quem financia, quem monta o roteiro, de onde saem as informações falsas que são ditas e repetidas e são impulsionadas. Isso aí é um problema absolutamente central. E onde reside a chave para esse problema? Entre outras coisas, na própria plataforma, porque se a plataforma opera de forma distinta...

Por exemplo, da mídia tradicional, que você sabe quem é o editor, quem é o relator, quem é o jornalista, que você pode processar, que você tem uma série de instâncias a que você pode recorrer e, numa plataforma dessas, até você passar por todas as instâncias - se é que você pode alçar todas essas instâncias - o dano já está feito, porque é em tempo real. Então, a gente tem uma situação extremamente assimétrica e bastante nociva ao processo democrático, que nós conhecemos e a que nós estamos habituados, todos aqui nesta sala. A gente está falando de uma outra coisa.

Vamos em frente.

Então, eu vou tentar só fechar aqui algumas ideias para haver depois uma discussão.

Pode passar, por favor.

Ah! Algumas propostas. Eu vou passar para o eslaide seguinte, porque eu acho ele mais simples. Esse aí.

Eu acho que tem algumas coisas têm que ser ditas desde já. Primeira coisa: ano que vem a gente vai ter uma eleição que vai ser basicamente com dinheiro público. Parte disso pode ser usado para impulsionamento. É importante que o dinheiro público não financie impulsionamento, que deturpe a eleição, que produza *fake news* e que, em última instância, atinja a própria democracia, a própria estrutura de Estado que financia o processo eleitoral. Eu acho que isso é do interesse da esquerda, da direita, do centro, não tem coloração partidária isso. Todos podem ser afetados, e não é justo que o dinheiro público sustente isso.

Então, é uma questão que tem que ser vista e tem que ser pensada e nós temos algumas discussões sobre isso. Só uma utilização de *block chains*, por exemplo, para seguir o dinheiro até a ponta - a ponta, eu digo, até a mensagem postada.

Outro ponto: responsabilização das plataformas. Absolutamente central. O WhatsApp, por exemplo, na última eleição, não tinha nem um escritório de representação no Brasil. Foram chamados pela Ministra Rosa Weber para discutir o que aconteceu nas eleições e eles tiveram que fazer uma teleconferência. E eu falo isso com muita tranquilidade. Eu participei do conselho que foi criado na época do Ministro Gilmar para fazer sugestões para o TSE sobre como lidar com esse fenômeno das *fake news*. Eu acho que o TSE tem que realmente implementar vigorosamente uma estrutura mais adequada para lidar com esse fenômeno, que vai distorcer bastante o processo eleitoral.

Análise de algoritmos: acho que pode ser feito não um acesso aos algoritmos, mas à resultante deles, o que pode ser discutido e pode ser feito. Hoje na Alemanha se faz isso. Acho que há centros no Brasil que podem fazer uma série de testes. Ainda que eles não sejam conclusivos, eles podem ser indicativos.

E finalmente a gente tem que pensar na...

A SRA. KÁTIA ABREU (PDT - TO. *Fora do microfone.*) - Não entendi. Como seria essa análise de algoritmos?

O SR. MARCO AURÉLIO RUEDIGER - Não há acesso a algoritmo das plataformas em absoluto, mas eu posso fazer uma série de testes de checagem, de forma uniforme, com vários centros fazendo os mesmos questionamentos, vendo as resultantes produzidas em resposta. É basicamente isso. Isso não é algo que possa, a partir daí, configurar o desvio, mas configurar um ponto de atenção.

Por exemplo, há pouco tempo isto circulou e era verificável: conteúdo altamente racista que vinha como resposta, por exemplo, no Google, a partir de perguntas aparentemente inocentes - por exemplo, mulheres negras dando aula. E vinha um conteúdo extremamente negativo. Como é que o algoritmo produz um negócio desse a partir de uma pergunta dessas? Então, esse tipo de coisa pode acontecer também no processo eleitoral. Não estou dizendo que há uma má-fé nas plataformas que geraram o algoritmo por detrás, mas, eventualmente, um indicativo desses por vários centros de pesquisa, ao mesmo tempo, sugere um olhar mais atento e um ajuste nisso durante o processo eleitoral.

Por fim, a proteção de dados. A gente tem uma lei de proteção de dados. Eu acho que a autoridade de proteção de dados tem que ser nomeada, essa lei tem que ser levada a sério, estão levando muito tempo para isso e eu acho que isso deve ter inclusive um desenvolvimento institucional na construção normativa da própria lei, ela tem que ser mais ampla ainda do que já é.

Com isso, eu basicamente encerro o que eu queria dizer para vocês.

Obrigado.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Vou passar a palavra para a nobre Relatora, Deputada Lídice da Mata, começar a fazer os seus questionamentos.

A SRA. LÍDICE DA MATA (PSB - BA. Como Relatora.) - Sr. Presidente, eu queria parabenizar os dois expositores, saudar todos os membros da Comissão, assessoria, imprensa e demais pessoas que nos acompanham.

Eu achei extremamente rica a exposição dos dois expositores. Primeiro porque está afirmado aqui, pela primeira vez, de forma peremptória, definitiva, que é confirmada por ambas exposições, que é possível se fazer o rastreamento. Está claramente aqui colocado, embora alguns outros tenham falado de dificuldades, está aqui claramente colocado isso. Segundo, que esse rastreamento pode ser feito através das empresas, ou seja, as empresas, as plataformas, diferente do que foi o comportamento de algumas frente à Justiça, devem ser estimuladas a fazer porque têm condições técnicas de viabilizar isso. Terceiro, aí já no nosso campo, no campo da sociedade, no campo da política, é que, mais do que estimuladas, essas empresas devem ser instadas a fazer isso quando necessário, quando a Justiça determinar, porque é um dever social que elas possam realizar essa tarefa, dever ético.

Eu quero fazer algumas perguntas rapidinhas apenas para confirmar essas coisas que destaquei.

Outra questão que achei importante e que foi destacada aqui pelo Dr. Marco Aurélio, que reafirma isso que falei aqui antes, que é a responsabilização das plataformas. Eu tenho insistido nisso desde o início desse nosso debate e pergunto aos debatedores que vêm, porque, com essa confirmação de como esse rastreamento pode ser feito, mais ainda é indispensável que nós possamos ter uma forma de responsabilização das plataformas.

Aí eu quero colocar uma pergunta ao Dr. Marco Aurélio: qual a metodologia utilizada para classificar um usuário do Twitter como robô? Se eles poderiam compartilhar com a CPMI, os dois, listagens de robôs identificados pela pesquisa?

Segundo, para os dois: como podemos ver nas palestras, é tecnicamente possível descobrir qual foi a primeira transmissão de uma imagem que contenha *fake news* no WhatsApp. É possível realizar uma investigação desse tipo sem ferir os dados privados daqueles que eventualmente retransmitiram tais imagens? Dr. Miguel, especialmente.

O senhor também afirmou ser possível identificar o IP do terminal que realizou o primeiro envio de uma mídia para o WhatsApp. Essa é uma informação suficiente para encontrar o usuário responsável pelo envio?

Na pesquisa que o senhor realizou, foi possível identificar a origem de postagem de *fake news* que circularam durante as eleições do ano passado. Durante a pesquisa, foi possível identificar a origem de postagens de *fake news* que circularam durante as eleições no ano passado?

Houve na pesquisa identificação de algum IP ou número de "zap" que tenha realizado o primeiro *upload* de dois ou mais conteúdos *fake*?

Tanto a PGR quanto a Polícia Federal confirmaram ter recebido relatório produzido pelo Sr. Miguel ainda no final do ano passado. Hoje, passado mais de um ano, algum desses órgãos entrou em contato com o senhor para solicitar informações adicionais ou fornecer respostas acerca da avaliação do seu relatório?

O senhor poderia compartilhar com esta CPMI o seu relatório e os dados utilizados para a sua confecção, garantido o sigilo dos dados sensíveis que eventualmente façam parte da pesquisa?

Nas informações para as autoridades policiais disponibilizadas pelo "zap", a plataforma afirma que não armazena mensagens uma vez que elas são entregues nem o registro de transação de tais mensagens entregues, contudo, nada é dito nesses termos sobre documentos, imagens, vídeos e outros tipos de mídias compartilhados pela plataforma. Existe diferença técnica entre o compartilhamento de mensagem de texto e o compartilhamento de arquivos de mídia?

E, para os dois, eu queria perguntar, com base também nessa discussão que temos visto ocorrer e acompanhado aqui na fala dos especialistas: uma vez solicitados a uma das plataformas, se não me engano o Facebook, dados para que pudesse participar de uma investigação, a resposta obtida é de que os dados não poderiam ser entregues porque eles não ficam armazenados no Brasil, mas sim no local de origem dessa empresa. Não seria, portanto, necessário que o Brasil pudesse decidir, exigir dessas empresas a instalação de espaços de reserva dos dados no próprio País, nos servidores aqui, no próprio País? Não seria o correto? Não parece um absurdo - perdoe-me a pergunta como uma pessoa não especialista no assunto -, não é absurdo que outro país possa ter acesso aos dados dos brasileiros e os brasileiros não possam ter acesso a esses dados, que nós não tenhamos servidores dessas plataformas aqui no País?

Para mim basta.

Presidente, como eu falei com o senhor ontem e comuniquei à CPMI, hoje eu devo me afastar um pouco mais cedo em função de uma viagem que faço para o congresso do meu partido.

Tenho que ficar aqui, provavelmente, só até às 4h30, mais ou menos, 5h, de maneira que, se, na oportunidade, eu tiver que sair e não houver acabado a reunião, eu solicito a V. Exa. que nomeie um Relator para esse período do meu afastamento, sem que os trabalhos possam ser prejudicados. Mas eu tenho a expectativa de que isso não precise acontecer.

Obrigada.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Você dirigiu as perguntas para os dois. Então, com a palavra o Dr. Miguel.

Pela ordem, Senadora Kátia Abreu.

A SRA. KÁTIA ABREU (PDT - TO. Pela ordem.) - Eu gostaria de propor e de pedir à Relatora, com todo o respeito, que a gente pudesse - são poucos Senadores aqui -, Deputada, fazer as perguntas, por conta de outros compromissos, mas são perguntas importantes, que a assessoria depois vai ouvir, e ela também, mesmo porque ela tem que sair, as respostas dos nossos questionamentos.

Quero saber se nós poderíamos fazer as nossas perguntas antes de ele responder a ela.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Tudo bem.

Então, V. Exa. tem alguma objeção, Senadora?

(Intervenção fora do microfone.)

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Então, vamos seguir a ordem dos inscritos aqui.

O primeiro inscrito aqui é o Deputado Paulo Ramos, a quem eu tenho o prazer de passar a palavra, porque, em todas as reuniões, ele é o último a falar, e desta vez ele abriu os trabalhos.

O SR. PAULO RAMOS (PDT - RJ. Para interpelar.) - Sr. Presidente, primeiro cumprimentar a todos, cumprimentar os expositores.

Eu poderia... Não vou usar uma expressão tão rigorosa comigo mesmo, mas eu não sou nem analfabeto digital nem conhecedor profundo, e tenho acompanhado aqui todas as exposições e vou me convencendo da complexidade. Até me lembrei de uma música do Zeca Baleiro. Diz:

Pra entender um trabalho tão moderno

É preciso ler o segundo caderno,

Calcular o produto bruto interno,

Multiplicar pelo valor das contas de água, luz e telefone...

E isso vai embora. Então, é uma complexidade muito grande, mas obviamente que é um comércio e, se é um comércio, comercializa-se. As empresas têm todo o interesse em ocultar, em vez de contribuir para a informação e as eventuais responsabilizações. Essa estrutura foi montada porque são informações extremamente relevantes, são procedimentos que podem se apropriar de toda a tecnologia, para o bem ou para o mal.

Nós, aqui... E a Deputada Lídice da Mata talvez tenha solicitado aquilo que pode contribuir para o trabalho da CPI, porque uma CPI, o nome já diz, é uma Comissão Parlamentar de Inquérito. Nós estamos diante de fatos já consumados, ilícitos praticados, e nós estamos também buscando a responsabilização de quem cometeu o crime.

Nós não estamos aqui num debate acadêmico para o aperfeiçoamento do sistema. Nós podemos até contribuir para o aperfeiçoamento do sistema, mas o objetivo principal da CPI é a investigação daquilo que foi praticado e que exige a responsabilização dos autores.

E, aí, a minha indagação talvez possa ser respondida pelos expositores, mas, se nós temos aqui uma afirmação de que é possível a identificação e nós temos, nos órgãos encarregados de investigação, profissionais completamente competentes - inclusive, a própria CPI solicitou a disponibilização de servidores públicos que são profissionalíssimos nessa matéria -, o que eu vou solicitar é que a Comissão Parlamentar de Inquérito indague aos órgãos que estão fazendo essa investigação se eles já chegaram a alguma conclusão, se eles já alcançaram um ou outro que tenha cometido esses ilícitos. Concordo que as empresas têm que ser responsabilizadas.

Vamos chegar a um ponto em que, enquanto não caírem no descrédito, as reputações vão sendo destruídas. Quem já foi vítima sabe o efeito que isso produz no universo frequentado por cada um. Na última eleição, por exemplo, eu fui vítima de forma tão agressiva e numa dimensão tão grande, que foi o fato escolhido pelo G1 para demonstrar uma *fake*. Um amigo meu chegou a me perguntar: "Você é candidato à Presidência da República?", porque vinha do Brasil inteiro!

Complementando então a intervenção da nossa Relatora, se eles têm conhecimento, mesmo antes da provocação da própria CPI - ou a Polícia Federal, o Ministério Público -, de alguma conclusão a que os órgãos de investigação já tenham chegado, alcançando uma ou outra das pessoas que eles já identificaram como responsáveis pela produção de *fakes*, influindo, obviamente - e foi a abordagem do segundo expositor -, no Estado democrático de direito, porque a eleição, o convencimento, a participação do eleitor se dá a partir do convencimento; quer dizer: a livre manifestação da vontade. O induzimento, a repetição de uma informação falsa, já que da Alemanha nazista vêm alguns exemplos, do Goebbels: "A mentira reproduzida muitas vezes se transforma em verdade".

Então, a minha indagação é se se tem conhecimento de alguém que já tenha sido identificado e a minha solicitação à CPI é encaminhar uma solicitação, para que nós possamos saber a quantas andam as investigações, porque o tempo está passando.

Temos aqui dados das eleições de 2014, nós temos as eleições de 2018, e estamos caminhando para as eleições de 2020, sabendo que, até lá, tudo estará igualmente incontrolável, a não ser que algumas providências mais radicais sejam tomadas.

Então, quero dizer que fiquei muito contemplado com as exposições, mesmo sem estar muito familiarizado com a dinâmica, a complexidade do tema, mas assumi uma compreensão de que nós estamos convivendo com vários riscos, com várias ameaças em relação ao Estado democrático de direito. Mas, aí, nós estamos diante também de um processo que está vinculado à legitimação do processo, à legitimação dos eleitos, em decorrência da vontade do povão, que é mobilizado às urnas para escolher seus representantes.

Obrigado.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Deputado Paulo, só para esclarecer a V. Exa.: já existem aqui, nos arquivos da CPMI, no cofre, aqui, vários inquéritos. Estão à disposição, inclusive, de V. Exa. e de sua assessoria. É só encaminhar os nomes, porque são sigilosos, e tem que marcar até horário para ter acesso pelo computador.

O SR. PAULO RAMOS (PDT - RJ) - Inquéritos já concluídos, com a identificação do...

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Não, ainda não. Estão em processo.

O SR. PAULO RAMOS (PDT - RJ) - A minha preocupação é que as coisas, às vezes, são muito lentas e...

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Mas aí nós temos que acionar o Ministério Público e o Polícia Federal, que são os órgãos investigativos.

O SR. PAULO RAMOS (PDT - RJ) - Para que eles digam se concluíram, pelo menos, porque é isto mesmo: o pior não é o travestido de sim; isto é, não conclui...

Houve um Governador, aqui do Distrito Federal - acho que foi o Arruda -, que resolveu fazer um decreto acabando com o gerúndio - acabando com o gerúndio. Nós não podemos ficar no "está sendo investigado...". Estamos investigando. Mas não conclui pela impossibilidade de concluir, não conclui pela incompetência ou não conclui pela cumplicidade? Não sei.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - É verdade.

O SR. PAULO RAMOS (PDT - RJ) - Obrigado, Senador.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Passo a palavra para a Senadora Kátia Abreu, do PDT, do Estado do Tocantins.

A SRA. KÁTIA ABREU (PDT - TO. Para interpelar.) - Muito obrigada, Presidente.

Este mundo, para mim... Eu tenho uma certa dificuldade; os filhos e os netos já têm toda facilidade. Mas eu vou fazer aqui uma pergunta, que pode até parecer primária, mas eu gostaria muito de achar solução para isso. Sei que não é simples.

Você, Dr. Miguel, acabou de dar aqui uma senha maravilhosa para o WhatsApp, de poder identificar o primeiro lançador de *fake news.* Então, vem exatamente coincidir com o que eu quero perguntar: como é que você vai superar essa dificuldade?

Quando eu compro um telefone pós-pago, Deputada Lídice, eu sou obrigada a ir presencialmente à empresa, apresentar meus documentos, compro meu pós-pago, ponho meu endereço e vou embora. A própria empresa faz isso, e registra, porque ela quer receber a sua conta de telefone pós-paga. No caso do *chip* pré-pago, eu só aciono a operadora, ativo com um CPF, por telefone, que necessariamente poderá não ser legítimo, poderá ser falso - eu usando o seu CPF, para lançar *fake news*. Então, o pré-pago permite você usar um CPF falso.

Nisso aqui eu paro e vou para a sua descoberta - certo? -: como é que você vai identificar esse cidadão? Você até pode identificar que ele enviou em primeira mão aquele *fake news. V*ocê vai chegar lá, o CPF é falso, óbvio, e você, então, não vai encontrar, porque nem endereço tem - ele vai colocar endereço falso também. Então, você só vai poder utilizar num pós-pago, e quem tem pós-pago dificilmente fará isso aqui. Ele vai comprar um pré-pago para fazer, para não ser identificado.

Bom, a outra questão é o Instagram, o Twitter e o Face. A mesma coisa: eu, para abrir essas redes, só preciso de um *e-mail* - qualquer *e-mail* -, que absolutamente não vai me identificar, que também não é presencial. Eu posso mencionar um CPF falso e, claro, posso mencionar um endereço também falso. E, como disse, o WhatsApp é a mesma coisa. Então, como é que nós vamos superar isso? No caso do telefone pós-pago, a pessoa tem que mostrar o rosto. E no caso do pré-pago?

Eu, com meu pequeninissimo conhecimento a respeito do assunto, zero de especialidade, penso que, no caso do pré-pago, tem que se encontrar uma solução para ele.

Eu sei que são milhares e milhares de pessoas que teriam que se dirigir às empresas para se identificar, e as empresas terão interesse nisso? Porque eu posso comprar um *chip* de R$10 e ficar com ele por três meses, sem aparecer o rosto, sem gastar mais nada.

Então, eu posso estar enganada, mas não é esse o grande "x" da questão? O telefone pré-pago, com dados falsos, e o *e-mail* falso, com endereço falso, para criar os três tipos de rede.

Esse era o meu questionamento.

Muito obrigada.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Deputada Bonavides com a palavra.

A SRA. NATÁLIA BONAVIDES (PT - RN. Para interpelar.) - Obrigada, Presidente.

Quero cumprimentar o senhor e nossa Relatora e também os nossos convidados, que trouxeram informações muito preciosas. Acho que nossa audiência pública de hoje está sendo muito importante para a nossa Comissão.

E eu queria destacar aqui essa metodologia apresentada por Miguel, porque, realmente, em muitas das oitivas, das audiências que a gente tem feito, a gente se depara sempre com essa dificuldade técnica, até pelo próprio discurso de empresas como o WhatsApp, que normalmente colocam, dizem haver ainda mais do que as que existem realmente. E eu acho que está posto que existe uma possibilidade técnica real de a gente fazer o rastreamento - pelo menos no WhatsApp - do início da disseminação dessas notícias. Eu acho que é uma metodologia muito preciosa que o senhor traz aqui para a Comissão e que pode nos ajudar a desbaratar essa rede de disseminação de notícias que a gente tem presenciado.

E, aí, diante disso, eu queria fazer algumas perguntas para os senhores.

Antes eu queria informar, Sr. Miguel, que o WhatsApp, num dos documentos que a gente solicitou aqui, por requerimento, e que foi respondido pela empresa, eles afirmaram que guardam por seis meses as informações. Então, eu vi na sua apresentação que havia essa dúvida, que eles mesmos chegaram, em algum momento, a dizer que não guardam, mas houve um requerimento que eles responderam, em que nós pedimos o relatório sobre os perfis que haviam sido bloqueados, no contexto das eleições de 2018, e eles afirmaram que só tinham aquelas informações por seis meses - por isso, neste momento da CPMI, já não tinham - e enviaram para nós o que eles, na época, conseguiram fornecer ao Tribunal Superior Eleitoral e, por isso, ainda tinham. Mas, pelo que a gente teve de informação, aqui na CPMI, sim, eles guardariam pelo período de seis meses também as informações.

Enfim, já passando aqui para as perguntas, eu queria saber se, pelo que vocês têm monitorado - e a gente percebe que vocês têm uma inserção nos grupos de Whatsapp -, aqueles que atuaram durante a eleição seguem atuando hoje em dia. Vocês percebem isso, se os grupos seguem ativos?

Eu também queria saber se vocês identificam que esses grupos e as mensagens que são passadas através deles seguem uma produção orgânica, espontânea, independente ou parece existir uma agenda comum, uma ação coordenada, uma ação centralizada, idealizada por algum grupo. Quero saber se existe uma coordenação centralizada, inclusive, entre grupos diferentes, se vocês conseguiram perceber isso, pelo que vocês têm monitorado.

Uma outra pergunta diz respeito à questão internacional.

A gente sabe que, no mundo inteiro, vários países estão se debruçando pelas mesmas questões que nós, aqui na CPMI, hoje estamos. No entanto, parece que, em alguns países, há diferenças, por óbvio. Por exemplo, a gente vê que, no Reino Unido, a maior preocupação lá foi, inicialmente, com o Facebook; e aqui, nas eleições brasileiras, nos pareceu que a maior preocupação foi com o Whatsapp. E o que eu queria perguntar é se aqui a gente está importando algum fenômeno ou, por essa diferença, pela própria utilização maior do WhatsApp, se é algo que parece que está surgindo aqui. Mesmo que a gente já esteja observando isso em outros países, é algo que parece ter começado aqui?

Eu não sei se os senhores estão familiarizados com o trabalho do Steve Bannon, nas eleições dos Estados Unidos, mas vocês enxergam alguma semelhança, alguma similaridade entre a forma como esse senhor atuou nas eleições estadunidenses e o que aconteceu aqui no Brasil?

E, por fim, vocês conseguem opinar se as pessoas que disseminam as notícias falsas nesses grupos, nessas mídias, parecem fazer isso enganadas, achando que estão reproduzindo conteúdo verdadeiro, ou parecem fazer isso sabendo que se trata de uma notícia falsa, mas que, embora sabendo isso, ainda assim, têm o interesse de espalhar a mentira?

E, por fim, quero saber a opinião de vocês sobre as chamadas *deepfake*. Isso é algo que requer uma tecnologia muito grande e que, por isso, ainda estaria longe de chegar a esse nível de interferência e de popularização? A gente sabe como é fácil e simples criar uma notícia falsa e disseminar, mas uma *deepfake* não é tão simples. Simular um vídeo, fazer um vídeo fazendo parecer que uma pessoa está falando algo que ela não está parece não ser tão simples, mas eu realmente não sei o quão não simples é. É algo que está longe da nossa realidade de disseminação em massa ou é algo que vocês estimam que, muito em breve, também vai chegar como um problema a ser enfrentado na nossa democracia e nos nossos processos eleitorais?

Eu encerro com isso.

Agradeço demais a participação de vocês aqui hoje.

E é isso.

Aguardo as respostas.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Passo a palavra ao penúltimo orador inscrito, o Senador Humberto Costa, para que, após isso, os nossos convidados possam começar a responder.

O SR. HUMBERTO COSTA (PT - PE. Para interpelar.) - Boa tarde a todos e a todas, aos nossos apresentadores...

Eu queria começar aqui pelo final da fala de Natália.

Eu até coloquei no grupo dos Senadores que integram a CPMI um vídeo que eu recebi - não sei se vocês viram, eu mandei - feito agora por uma entidade, uma ONG que trata de notícias falsas no Futura e tal. O que eles simulam é um negócio de uma perfeição tão assustadora...

Então, nesse vídeo... Era como se fosse um vídeo produzido pela BBC - há lá a marquinha da BBC -, e, de um lado, está o Ben Johnson pedindo votos para o Corbyn, que é trabalhista, e o Corbyn pedindo votos para o Ben Johnson. E eles mostram como é que se construiu aquele vídeo de *deepfake*. E não parece ser uma coisa tão complexa não, viu? Eu fiquei assustado, porque é perfeito, é uma coisa perfeita, e aí eles mostram todas as fases, como foram feitas, até chegar ao momento de uma pessoa que imita os movimentos da boca de cada um deles. Olha, é um negócio realmente preocupante.

Mas eu queria fazer algumas breves perguntas. Uma delas é o seguinte... Sobre grupos de Whatsapp.

Em muitos deles, há as pessoas que criaram, e essas pessoas mantém 20, 30, 40 ou até 50 grupos ao mesmo tempo, todos preenchidos com pessoas que não se conhecem entre si, mas com a mesma vertente política. Aí, a pergunta é: dentro desse contexto, é justo tratar tais grupos de WhatsApp como comunidades entre particulares, sendo as mensagens ali trocadas diálogos entre particulares que devem ser protegidos pelo direito à intimidade, ou tais grupos mais se assemelham à comunicação em massa, devendo ser tutelados por legislação de mesma natureza das que se observam em meios de comunicação tradicionais?

A outra é: os senhores enxergam a possibilidade de formular regulamentações sobre *fake news* nas redes sociais como sendo uma forma de reduzir a democracia, a liberdade de expressão?

Pergunta três: há alguma ligação entre grupos de WhatsApp, do que os senhores têm conhecimento, que propagam notícias falsas e *sites* que são conhecidos por propagarem notícias falsas?

E, por último, quero saber se vocês têm informação se, antes do período eleitoral de 2018, houve algum momento político em que se observou a proliferação intensa de notícias falsas? O período, por exemplo, que antecedeu o impedimento da Presidenta Dilma Rousseff registrou algum tipo de anormalidade?

Seriam essas.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Passo a palavra agora ao Senador Rogério Carvalho, do PT, do Estado de Sergipe, último orador inscrito, antes de passarmos a palavra para os dois convidados.

O SR. ROGÉRIO CARVALHO (PT - SE. Para interpelar.) - Eu cheguei um pouco atrasado, mas já me deram conta de que o Sr. Miguel de Andrade Freitas disse que é possível identificar o primeiro disparo de WhatsApp. Como também já foi dito aqui, o Whatsapp, nessas eleições, foi a rede preferencial para se chegar aos eleitores, não só com *fake news*, mas também com comunicação dirigida.

A gente, às vezes, se perde um pouco no debate de *fake news* e não discute o fato de você ter instrumentos e acesso a bancos de dados para produzir uma comunicação dirigida de acordo com a suscetibilidade, a vulnerabilidade, as características das pessoas, o que é possível com os *big datas* que existem e as metodologias de aproximação de perfis e de suscetibilidades, com a psicometria que eles adotam e que adotaram no Brexit, que adotaram na eleição do Trump, que adotaram em eleições que serviram de piloto no Brasil. Ninguém fala, mas há suspeitas de que a eleição da cidade de São Paulo também teve o primeiro treino e a primeira utilização, em menor escala, do que foi utilizado na eleição presidencial. Eu falo da eleição da Prefeitura de São Paulo em 2016, que estava no bojo.

E vejam: há o fenômeno, que eu acho que é importante. Então, eu vou fazer uma pergunta, aí, ao Presidente da Comissão, à Relatora, e sob sua orientação: como se ter acesso a essa primeira mensagem? O que que a gente precisa fazer? Quais são os instrumentos que a gente precisa adotar para ter acesso a isso? No caso - e é isto que deve acontecer - de o Facebook dizer ou que não tem... Mas a gente sabe que tudo fica registrado. É muito difícil... Só se eles fizeram a destruição física do lugar onde armazenavam essas informações; senão, elas estão lá - comprimidas, mas estão lá. Não sei se isso é verdade, mas o senhor, como técnico, pode responder para a gente. Só se eles destruíram o equipamento físico onde estão guardadas. Só se eles destruíram. Se não destruíram, está lá, comprimido. Comprimiram a tal ponto que não se consiga descomprimir, com tanto dado que já foi colocado ali, intencionalmente.

Também é possível saber se eles aumentaram o volume sobre aquele equipamento específico para comprimir a informação, a ponto de você não conseguir capturar a informação de volta.

Então, como a gente consegue fazer isso? Essa é a primeira questão.

E, aí, para o Presidente e para a nossa Relatora: que caminho nós vamos seguir para chegar lá?

A segunda questão...

Eu não vi a palestra - eu estava na sessão do Congresso, cheguei atrasado. Então, eu peço desculpas. Mas, na minha opinião - e eu queria saber a opinião de vocês -, tão ruim quanto a *fake news* são as comunicações dirigidas, porque...

Deputada Lídice da Mata, eu fui candidato, no meu Estado, tenho uma história de militância política de 33 anos, já exerci vários mandatos - fui secretário municipal, fui secretário estadual... Então, sou uma pessoa que teve uma vida bastante atribulada e muito conhecida. E eu era votado - fui votado -, em Municípios pequenos, porque eu tinha obra, porque eu conhecia aquele Município, porque as pessoas me conheciam, porque eu tinha relação.

Agora, como se explicam candidatos, com menos de dois anos de exposição real, terem voto nesses Municípios sem nunca terem colocado os pés nesses Municípios?

Então, aí alguma coisa há a mais. Não só *fake news* é o problema, é como eu acesso bancos de dados que me permitem chegar a todas as pessoas que me interessam e fazer uma comunicação dirigida, sem que essa comunicação tenha contraponto. Então, isso, como disse o Humberto, é um crime para a democracia! Como é que eu coloco uma opinião que só você está vendo e eu coloco outra opinião completamente diferente para Lídice da Mata, que é antagônica a que eu mandei para você, mas só ela vê? Então, não há contraponto, não há contradição. Você faz uma campanha em que as pessoas não sabem quem é você, elas só sabem o que você disse, porque você disse o que elas queriam ouvir ou o que algum algoritmo disse que aquelas pessoas, pelas informações sobre aquelas pessoas, gostariam de ouvir. O algoritmo diz que aquela pessoa gostaria de ouvir aquele assunto e não outro assunto. Então, você consegue não só, com essas ferramentas todas... Estamos focados em *fake news*, mas nós temos um grande mal...

Fake news é uma mensagem que diz assim à Dona Lídice, tomando a senhora como exemplo de uma eleitora: "Dona Lídice, esse candidato bate em mulheres". Isso chegou à senhora, que é feminista, que tem uma história de militância, e, se aquele candidato bate em mulheres, a senhora quer ver o satanás e não quer ver esse candidato. Por quê? Porque não dialoga com a sua história. Agora, como chegou a isso de que a Dona Lídice é feminista? Ele teve acesso a algum banco de dados, algum instrumento foi adotado.

Eu acho que a gente precisa olhar para *fake news*, mas olhar para que bancos de dados foram adotados para disparar *fake news*. Que tecnologias de análise desses bancos de dados foram adotadas? Foi a tecnologia da Cambridge ou foi a daquela empresa cujo nome citei aqui ontem, ou daquela pessoa cujo nome citei aqui ontem? O Ba Assunção? A informação que eu tenho é que ele preparava, de acordo com o algoritmo, a mensagem que deveria ser encaminhada para determinados grupos. Aí ele preparava *fake news* ou *news*, não importa. O que importa é o modo como chega; e chega de forma dirigida, sem contraponto; e chega para o Sr. Miguel de uma forma, para a Dona Lídice, de outra forma, para o Sr. Marco de outra maneira, ou seja, são conteúdos distintos, que não se contradizem. É como se eu botasse um atirador de elite diante de um alvo a 100m: quantos tiros esse atirador a 100m do alvo, com uma arma de precisão, vai errar? Nenhum. Agora, se eu botar a 100m um exímio atirador com uma pistola, quantos tiros ele vai acertar no alvo? Poucos, pois são muitas variáveis que interferem.

Então, hoje, eu sou analógico; V. Exa., Deputada Lídice, é analógica; V. Exa., Senador Angelo Coronel, é analógico. Sabem por quê? Porque a gente fala como se fosse nas ondas da rádio, a gente faz um discurso difuso, mas eles não usaram esse tipo de tecnologia, eles usaram um tipo de tecnologia dirigida.

Aí a paridade de armas deixou de existir na eleição. Só isso já seria suficiente para anular qualquer eleição! Esse mecanismo faz uma separação entre as capacidades... Interferiu no resultado da eleição! Não é assim que se julga no TRE, no TSE quando se vai fazer um julgamento? Qual é o julgamento que se faz? Abuso de poder econômico. Aí se cassa um indivíduo que ganhou a eleição, porque ele abusou do poder econômico. Por quê? Porque a paridade de armas não foi compatível entre os demais candidatos. Abuso do poder político. Aí a não paridade de armas obriga a cassação daquela candidatura vitoriosa, porque a vitória foi contaminada pela paridade de armas que não houve.

Eu pergunto: se alguém tem acesso a bancos de dados ilegal, se alguém adota metodologias dessa natureza, porque elas estão disponíveis e foram utilizadas por vários candidatos, isso não é suficiente? Não há diferença entre paridades de armas para disputa eleitoral? Isso é democrático?

São essas questões e essa reflexão que eu gostaria de deixar, retornando para V. Sas.: o que fazer e como chegar a eles? A que mecanismo a gente pode chegar, para orientar aqui o nosso Presidente e a nossa Relatora?

Obrigado.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Passo a palavra agora para os dois convidados, dois técnicos, que eu tenho certeza de que vão responder às perguntas bastante pertinentes dos nobres Parlamentares.

Com a palavra o Dr. Marco.

O SR. MARCO AURÉLIO RUEDIGER (Para expor.) - Eu queria estabelecer aqui, em primeiro lugar, em termos conceituais, uma coisa, pois eu acho que, usando uma forma muito popular de se falar, todo mundo tem que cair na real: as eleições como elas existiam não vão existir mais. A gente está no novo normal. Isso não é um ponto fora da curva, é uma nova curva. Eu acho que isso tem que ficar muito claro. E não necessariamente isso é uma coisa ruim, porque, na verdade, as redes surgem com vigor com uma expectativa bastante utópica de construção de consensos, de ampliação do fluxo de informações e de diminuição de assimetria de informação e tal... Isso ainda é possível, mas o que veio, digamos assim, de contrabando nisso, que é ruim, é o fenômeno que a gente vive com redes, com robôs, com *fake news*, com desinformação em massa etc. Então, a gente tem esses dois lados e a gente tem que tomar muito cuidado quando se pensa em qualquer tipo de regulação. Evidentemente, alguma regulação tem que ser feita.

Se a gente olha, por exemplo, o TSE, os TREs hoje e retroage no tempo, eles fazem um trabalho bastante importante, que a gente tem que aplaudir, com as urnas, com o processo de votação etc., mas eles estão, de fato, preparados para essa nova realidade? Eu julgo que não, eu acho que existe um déficit de capacidade institucional muito sério hoje na Justiça Eleitoral. E isso tem que ser resolvido, como no passado foram resolvidos outros problemas na sociedade brasileira, com investimentos em desenvolvimento institucional. Isso é uma coisa que tem que ser feita. Eu acho que isso é do interesse de todos os campos políticos. Ainda que um campo político hoje possa ter uma capacidade operacional muito maior nas redes que outro, isso não vai ser para sempre assim, isso pode mudar. Então, essa regra tem que ter uma visão cívica, republicana mesmo. Eu acho que esse é um ponto muito importante aqui, em que eu acho que a Comissão tem que se debruçar, que tem que reforçar. Então, esse é o primeiro ponto.

O segundo é o seguinte. A eleição, em termos de rede, é em tempo real. E os processos de se vislumbrar, de se questionar, de se punir são analógicos, operam de forma analógica. Há uma contradição temporal aí extremamente séria, que não está resolvida.

Voltando às perguntas que houve - eu quis fazer esse preâmbulo -, há uma pergunta importante, que eu acho que foi da Deputada Natália, sobre se os grupos estão ativos ainda. Sim. Não há mais o que dizer. Basta você entrar nesses grupos que você vai ver. Se eles são coordenados... Eu acho que, provavelmente, subsistem de forma bastante coordenada. Não estou dizendo que todos são assim, mas que existem assim. Basta você entrar e participar que você vai ver que, em algum ponto, alguns não vão ser coordenados, mas muitos são coordenados. Dados empíricos podem mostrar isso.

Eu diria até - e esta é uma observação importante - que, se pegarmos, por exemplo, a lei de proteção de dados da Alemanha, o que se faz hoje para fazer aferição do Whatsapp não seria nem permitido. Então, a gente tem que se debruçar muito sobre a questão de proteção de dados em geral, porque isso vai colidir diretamente com o direito de a pessoa se expressar. Essa é uma questão muito importante que foi endereçada aqui, e de que vou falar daqui a pouco, pelo Senador Humberto Costa, que comentou isso há pouco. Essa é uma questão central.

A questão internacional. Eu não acho que Steve Bannon promova essa operação aqui no Brasil, porque ele está interessado na Europa, na Itália, na França, na Alemanha, mas eu acho que, de certa forma, ele é um mentor de uma visão de mundo que é muito radicalizada e que transcende o campo conservador, vai muito além do campo conservador, vai para um campo extremo, que é altamente nocivo à democracia, na minha opinião. Quanto a isso, eu acho, sim, que a gente tem que abrir o olho, mas eu não acho que ele opere isso aqui dentro. Eu acho que os brasileiros operam essas coisas aqui e talvez tenham diálogos fora, mas, basicamente, as estruturas são aqui. É a impressão que eu tenho sobre isso.

Deepfake news. Outra coisa importante. Neste ano, eu estive numa conferência em Copenhague, e essa conferência teve como *sponsor* uma série de organizações internacionais. Eu fui lá como membro do Design for Democracy, que é um segmento do National Democratic Institute, e ela aconteceu na mesma época do G20, e, no G20, estava o Presidente dos Estados Unidos etc. Então, abriu dizendo: "Infelizmente um dos convidados não pôde vir, porque está no G20, mas vamos falar com ele por teleconferência", e abriu na tela o selo da Presidência americana com depois o Donald Trump falando. E ele respondia absolutamente de uma forma coerente com o discurso dele normalmente. No final, eles falaram: "Vocês acabaram de assistir a uma *deep fake news*: todo o discurso está lastreado em inteligência artificial. Isso aqui não foi verdadeiro, foi montado para mostrar o impacto da tecnologia no processo político daqui para frente".

Bom, *deep fake news*, nenhum de nós tem condição de, a olho nu, entender o que é *deep fake news*, a gente vai achar que isso é verdade, só com determinados mecanismos muito mais sofisticados e tecnológicos. Isso é uma coisa que a gente vai ter que enfrentar. De novo, eu volto no meu ponto: a gente tem que ter um desenvolvimento das estruturas institucionais do País que são vinculadas à questão da promoção não só de uma forma *fair* de utilização das redes, mas também da proteção de dados etc. Então, isso para mim é extremamente central.

Uma pergunta aqui que eu acho que foi fundamental também e que me chama atenção é sobre o direito de as pessoas se expressarem. Essa é uma questão central, eu acho que essa é uma questão que veio aqui já a este Plenário várias vezes. Eu

tenho o direito, como cidadão, de exprimir minha opinião. Então, essa é uma questão. Essa é uma questão cuja reflexão que eu trago para vocês tem uma série de autores: o Popper, o John Rawls e outros autores, enfim, vão discutir sobre os limites da tolerância aos intolerantes. Eu acho que é nestes termos que tem que ser feita essa discussão. É evidente que as pessoas não podem ser cerceadas no seu direito de expressão, mas esse direito de expressão tem um limite de ser tolerado na medida em que ele destrói as bases que permitem o próprio direito de expressão. É quase um paradoxo da democracia, mas é uma coisa sobre a qual tem que se refletir. Então, não é possível se pleitear no âmbito das redes uma liberdade absoluta, até em termos em que é danosa aos próprios princípios que constam na Carta Constitucional, e depois se endereçarem propostas que não são coadunadas com esse próprio princípio no mundo real. Eu não quero ser muito mais explícito do que isso, mas acho que deu para todos entenderem. Então, eu acho que essa é uma questão importante, uma questão de fundo e tem que fazer parte das discussões aqui, nestes termos, até porque existem juramentos e compromissos, e a quebra disso é perjúrio.

Uma questão daqui da Cambridge Analytica que foi basicamente *microtargeting* de novo: boa parte das questões que estão aqui sendo vistas depende bastante da regulação e da questão das plataformas. As plataformas têm que ser mais *accountable*.

Eu acho que o direito à privacidade é o.k., mas elas podem anonimizar e, ao mesmo tempo, coibir determinadas práticas. Eu acho que isso é importante, o Brasil tem que fazer isso. Se eu não me engano, a Senadora Kátia Abreu falou alguma coisa sobre a base de dados.

(Intervenção fora do microfone.)

O SR. MARCO AURÉLIO RUEDIGER - Não foi a Senadora? Foi a Deputada Lídice que falou.

Eu acho que é o seguinte: não importa muito onde o banco de dados vai ficar, mas, por exemplo, na legislação europeia - salvo melhor juízo, posso incorrer num equívoco aqui -, me parece que a questão toda está no seguinte: os dados dos cidadãos europeus podem ser, de alguma forma, vinculados à legislação de proteção de dados da Europa, e isso é dado no âmbito democrático dos países europeus. Não importa onde os dados estejam. E as empresas são, portanto, atadas a isso, uma vez que elas operam na Europa. Então, eu acho que a gente tem que pensar nesses termos também para o Brasil.

Eu acho que um diálogo entre o Brasil e Europa é bastante importante nesse sentido, porque a discussão lá está bastante rica, muito embora eu diga que também nos Estados Unidos está sendo uma discussão muito contundente, muito forte e muito rica neste momento. Isso não atinge apenas a nós, essa é uma questão global, de fato.

Sobre a existência de interferência externa, eu não tenho dúvida de que existe também alguma interferência externa nesse processo - nós mesmos identificamos várias vezes isso, publicamos isso, inclusive não é nenhum dado secreto -, mas eu não acho que essa interferência externa seja relevante suficientemente para alterar qualquer tipo de resultado ou para distorcer a tal ponto os processos democráticos, eleitorais, de debates, de discurso. Isso é feito internamente. De novo, eu acho que aquele *app* do sistema do YouTube é muito importante ser vislumbrado e ser regrado. Eu acho que as regras que cabem para a mídia deviam ser, de alguma forma, adaptadas para isso. De onde vem o dinheiro que sustenta uma série de canais? Quem financia isso? Que tipo de informação está se vinculando lá, que pode ser absolutamente não verdadeira e danosa? Nisso também tem que haver uma observação em cima. E, de novo, a gente cai em: quem faz isso, quem regula isso, quem observa isso, dentro dos parâmetros e todo o respeito necessário às liberdades democráticas que constam da nossa Carta Constitucional.

Dito isso, a nossa metodologia está aberta. Eu posso encaminhar depois aqui para a Presidência da Comissão, na CPMI, a nossa metodologia e colaborar no que for necessário sobre os dados.

Por fim, o último ponto: eu acho que a discussão é muito centrada - e é muito importante que seja - no que passou, mas eu acho que tem que se preocupar muito com o que vem. E o que vem pela frente é muito pior do que se passou. Uma eleição com cinco mil Municípios - só pegando as regiões metropolitanas, estamos falando de 500 grandes cidades - é uma coisa extremamente preocupante na medida em que a gente está basicamente não instrumentalizado da forma adequada para lidar com isso.

É o que eu queria dizer, cumprindo a minha participação aqui.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Passo a palavra para o Dr. Miguel Freitas.

O SR. MIGUEL DE ANDRADE FREITAS (Para expor.) - Obrigado, Presidente.

Eu acho que foram perguntas bastante interessantes que vão ajudar a esclarecer uma série de questões. Eu vou pela ordem, então vou começar pelas perguntas da Relatora, Deputada Lídice.

Sobre a questão da responsabilização, eu acho sempre complicado você responsabilizar... É a velha discussão, especialmente no caso do WhatsApp, que se coloca muito como uma ferramenta de comunicação pessoal. Você

responsabilizar a ferramenta pelo conteúdo... Eu acho que a responsabilização mais direta é aquela que já está prevista em lei, por exemplo, em termos do Marco Civil, ou seja, eles têm a obrigação de atender a uma requisição judicial, a uma requisição legal de fornecimento de determinadas informações. No caso, por exemplo, de páginas no Facebook, também existe. Quando você tem um caso eleitoral, o juiz geralmente dá uma liminar de que a página tem que ser retirada do ar em tantas horas.

Então, eu vejo muito essa responsabilização em cumprir o que já está tipificado e especificado, e não especificamente uma responsabilização pelo conteúdo que trafega. Eu acho que isso é bastante complicado.

Se a metodologia que eu propus protege a privacidade dos dados de quem retransmitiu... Na verdade, ela nem consegue acessar esses dados, porque o processo de você retransmitir uma mídia no WhatsApp, de certa forma, não tem muito controle por parte da empresa. Eu posso pegar aquelas duas referências que eu coloquei na minha apresentação, que é a URL de onde o arquivo criptografado está hospedado no servidor da empresa, e eu posso pegar a senha que eu uso para descriptografar esse arquivo - posso pegar aqui -, anotar num papel e entregar para qualquer pessoa, quer dizer, não há como você ter controle de como essa informação circula dentro da plataforma, porque, quando ela circula dentro da plataforma, aí, sim, ela está dentro da mensagem, que é criptografada fim a fim - e o WhatsApp não tem acesso. Se ela circular por fora da plataforma, aí mesmo é que não tem acesso.

Naquele *link* que eu coloquei de exemplo na minha apresentação, eu fiz um *copy and paste* na janela do *browser* ontem de noite e eu baixei o arquivo, quer dizer, eu baixei aquele arquivo criptografado sem usar o WhatsApp. Então, tudo bem, o WhatsApp sabe o meu IP, mas ele não vincula isso necessariamente a uma conta de um usuário que está compartilhando aquela mensagem ou lendo aquela mensagem. Eu vejo uma questão muito mais forte de quando o arquivo é criado, porque, quando o arquivo é criado, ele sabe para qual usuário ele deu a permissão de fazer o *upload* daquele arquivo, daquela mídia - que, no caso, é criptografada, mas a gente pode ter recebido aquela mídia por mensagem e saber ao que aquela mídia corresponde -, e ele sabe o IP e hora de onde partiu aquela conexão, que, na verdade, é a sua pergunta seguinte, sobre se o IP seria suficiente para localizar o autor - isso também é parte da pergunta da Senadora Kátia.

Geralmente, como é que funcionam essas investigações? E aí eu estou propondo uma metodologia para o WhatsApp, mas é a mesma metodologia que é usada em qualquer página - num blogue, num Facebook. Eu só estou dando um detalhe técnico, que não era de conhecimento geral, mas existem exemplos na Justiça em que você identifica um conteúdo criminoso - seja calúnia, seja pedofilia - que está hospedado numa certa página, num blogue, num Facebook e você solicita para o provedor de aplicação os registros de conexão que foram responsáveis pelo *upload* daquela mídia para a plataforma. Então, o provedor de aplicação fornece essa informação.

Ele retorna: "Esse *upload* partiu do IP tal, no dia tal, em certa hora". Essa informação tem que ser levada para a operadora - por exemplo, para a Telefônica, para a Vivo, para a TIM -, e você pergunta para a operadora: "Operadora, quem era o terminal que estava usando esse IP nessa hora?". Porque os IPs são dinâmicos - a maioria, há IPs fixos também; mas a maioria dos IPs são dinâmicos. Então, a operadora vai informar: "Não, isso aqui partiu dessa conexão", e, em alguns casos, é uma conexão residencial, você pode chegar à casa da pessoa.

Então, essa questão, de certa forma, dialoga com a dúvida da Senadora Kátia sobre a questão do pré, do pós-pago, do CPF. É claro, o pré-pago, com CPF...

A SRA. NATÁLIA BONAVIDES (PT - RN. Para interpelar.) - O senhor sabe dizer por quanto tempo as operadoras guardam esse registro? Se também apagam, como as redes?

O SR. MIGUEL DE ANDRADE FREITAS - Isso está no Marco Civil, eu não me lembro. É outro artigo do Marco Civil. Eu não me lembro se é mais ou menos de seis meses, mas isso está...

A SRA. NATÁLIA BONAVIDES (PT - RN. Para interpelar.) - Só mais uma pergunta, desculpa atrapalhar o raciocínio.

O senhor falou sobre o IP poder localizar uma conexão que esteja ligada a uma residência, por exemplo. E, no caso do celular, o IP dá que informações sobre a conexão de celular?

O SR. MIGUEL DE ANDRADE FREITAS - Aí dá informação do número que estava com o IP naquele momento.

A SRA. NATÁLIA BONAVIDES (PT - RN) - Nada sobre localização?

O SR. MIGUEL DE ANDRADE FREITAS - Sobre a localização, dá aproximadamente, você diz a célula do celular, então você tem a região em que a pessoa estava...

A SRA. NATÁLIA BONAVIDES (PT - RN) - Em que antenas?

O SR. MIGUEL DE ANDRADE FREITAS (Para expor.) - Em que antenas, exatamente.

Agora, um usuário malicioso, mais sofisticado pode usar mecanismos para tentar se esconder melhor, quer dizer, é uma coisa simples. Você pode entrar numa cafeteria, numa livraria, usar uma *wi-fi* de certa forma pública, e essa operação não está vinculada à sua residência; quer dizer, depois você pode, numa investigação, olhar a câmera da cafeteria, olhar a câmera da livraria? Pode, mas é sempre um processo de investigação que tem esses caminhos, assim como o caso de que a Senadora Kátia falou do CPF falso. Se você tem um cartão pré-pago com CPF falso, você tem essa localização aproximada de onde a pessoa estava usando, mas não necessariamente por que a pessoa usou um CPF falso e um pré-pago para se cadastrar no WhatsApp ela é não localizável, porque ela pode muito bem ligar a *wi-fi* e acessar de casa. Então, é interessante e, na verdade, é importante para o caso do WhatsApp: o número telefônico que está associado àquela conta não diz muita coisa, porque tudo que você precisa da linha telefônica é para fazer o registro inicial do WhatsApp. Você pede um registro e você fala: "Meu número de telefone é esse". O WhatsApp vai mandar uma confirmação via SMS e, se você confirmar, aquele registro, aquela associação àquele número é feita. A partir daí, você pode pegar *o chip* e destruir e fica utilizando só no *wi-fi*, é uma possibilidade. Então, eventualmente o WhatsApp pode querer reconfirmar? Pode, mas, enfim...

Na questão da automatização, quando você tem os disparos em massa com o WhatsApp, você não está fazendo um disparo em massa usando esse mesmo aplicativo de WhatsApp que a gente tem no celular; são empresas que usam *softwares* que foram feitos a partir de engenharia reversa do protocolo do WhatsApp. Quer dizer, da mesma forma que eu analisei o protocolo do WhatsApp para trazer aqui detalhes de como funciona, uma pessoa que tenha feito essa engenharia reversa poderia investir em desenvolver um clone do cliente do WhatsApp e, com esse clone do cliente do WhatsApp, ela pode, por exemplo, de um computador, dizer que está registrada com cem linhas telefônicas diferentes. Então, você tem uma plataforma dedicada a fazer o envio massivo de mensagens no WhatsApp que não é um celular, é uma outra coisa, é de um outro bicho de que a gente está falando e que é feito especificamente para isso.

Continuando aqui nas perguntas, a Relatora perguntou se houve identificação no IP, e aí eu preciso esclarecer que a metodologia que eu propus e a análise das mensagens que eu fiz não chegaram ao IP. Para chegar ao IP, é necessária uma ordem judicial, e eu não tenho isso. O que eu mostrei é, como na apresentação, uma URL de um arquivo que corresponde a uma determinada imagem. Esse arquivo propagou nas redes e tem um criador, mas só quem sabe quem foi o criador desse arquivo é o WhatsApp. Eu não tenho essa informação. Eu só chego apenas ao nível da URL, ou seja, ao mesmo nível a que você chegaria se você fosse denunciar uma página do Facebook para a Justiça. Eu vou chegar para a Justiça e falar: "Olha, essa página aqui está cometendo esse crime, e o endereço dessa página é esse". Então, é basicamente o mesmo nível a que eu posso chegar por conta própria nessa metodologia que eu estou propondo.

Se a Polícia Federal entrou em contato com relação aos dados que eu compartilhei, não.

Se eu posso compartilhar os dados sob sigilo com a Comissão, eu posso compartilhar, eu já compartilhei, Presidente, o relatório que tem um resumo, mas eu posso compartilhar os dados mais detalhados, com as planilhas de propagação das mensagens, desde que isso seja guardado com sigilo pela Comissão, não há problema.

Havia a pergunta também sobre a resposta do WhatsApp de que ele não armazena transações, mas mantém os arquivos. Essa é uma pergunta interessante, porque pode ser que eles não armazenem as transações - quer dizer, as transações aqui seriam os registros de quem fez o *upload* daquele arquivo -, mas mantenham o arquivo em si. Isso é possível que seja. Esse arquivo, por exemplo, que eu acessei ontem já tem um ano que está hospedado lá nos servidores do WhatsApp e não foi apagado. Se você ler os termos de uso do WhatsApp, diz-se que eles podem manter, se eu não me engano, por um mês, e eles argumentam que eles fazem isso com o efeito de otimizar o funcionamento da rede. Então, esta realmente é uma questão técnica: ele armazena aquele arquivo durante um mês - quer dizer, ele diz que pode armazenar durante um mês, mas na prática pode permanecer por períodos maiores ou eventualmente menores -, mas com o objetivo de otimizar, ou seja, quando eu fizer uma retransmissão, um encaminhamento daquele conteúdo, eu não preciso fazer o *upload*. Então, é interessante ver que essa metodologia que eu estou propondo se baseia no fato de que dá escalabilidade para a plataforma do WhatsApp, quer dizer, é uma decisão de projeto do WhatsApp que eles tomaram para que a experiência do usuário seja mais eficiente: quando ele encaminha, o encaminhamento é instantâneo, ele não tem que gastar o pacote de dados dele para reenviar aquele conteúdo para fazer um encaminhamento. Então, essa é uma observação.

O Deputado Paulo Ramos perguntou sobre a questão de investigar e contribuir para o aprimoramento. Eu realmente não sei, decorrido esse tempo, pela questão dos registros, se estão preservados; se a investigação ainda consegue resgatar essas informações. Isso realmente só o WhatsApp vai poder dizer. Isso realmente só o WhatsApp vai poder dizer, mas eu acho que o trabalho pode contribuir para um aprimoramento também, porque pode se estabelecer um processo com essas provedoras de aplicações em que, para um caso futuro de uma investigação criminal, você já tenha as instituições - a polícia, Ministério Público, todas as instituições - cientes de formas efetivas de investigação e saibam que podem ter a colaboração das empresas para avançar com essas investigações. Então, eu pessoalmente enxergo uma oportunidade de

aprimoramento, sim, para casos futuros, para que os crimes de que a gente tem notícia e que podem ser motivados por *fake news* não se restrinjam às eleições. A gente tem casos aí de linchamento. Houve uma mulher no Guarujá, se eu não me engano, que foi linchada...

(Intervenção fora do microfone.)

O SR. MIGUEL DE ANDRADE FREITAS - Santos? No México, houve casos horríveis de pessoas que foram incendiadas, na Índia, então, esse é o um problema global. Eu acho que é possível aprimorar esses mecanismos de investigação para haver mais responsabilização.

Completando também, eu não investiguei pessoas. É aquela resposta que eu já dei com relação à metodologia. A metodologia identifica a página, quer dizer, a URL que hospeda aquele conteúdo que a gente consegue ver que é uma *fake news*, porque a gente recebeu essa mensagem num grupo.

Quero chamar a atenção a um detalhe, pelos dados que vão ser compartilhados com a Comissão: quando a gente apresenta, por exemplo, uma planilha e a gente mostra como uma mensagem, mesmo que seja uma mensagem falsa, circulou nos grupos que a gente monitorou, isso tem que ser visto sempre como uma amostragem num universo muito maior. Então, não é porque eu tenho determinado telefone que mandou primeiro aquela mensagem que aquele telefone é o autor. Aquele telefone é a primeira pessoa que compartilhou aquela mensagem, aquela mídia dentro do subconjunto que foi amostrado. Então, é importante não confundir as duas coisas. É por isso que a minha metodologia vai na questão do *upload* do arquivo, quando a gente identifica que é uma mídia que circulou em todos os grupos, preservando a mesma URL, que indica que são todos compartilhamentos de uma mesma transmissão inicial para a plataforma.

À Senadora Kátia eu já respondi a questão do pré-pago, do pós-pago, do CPF falso.

Deputada Bonevides, queria destacar aqui que a metodologia é limitada ao que se propaga na plataforma do WhatsApp. Então, se você tem uma produção de conteúdo falso, eu envio esse conteúdo falso para uma outra pessoa por *e-mail* e essa segunda pessoa que vai fazer o *upload* para a plataforma, quem vai aparecer é essa segunda pessoa, não necessariamente quem foi que fez o Photoshop ou o que seja. É interessante essa resposta do WhatsApp de que eles guardam por seis meses, porque é diferente da resposta que eles deram para a *Folha* no início do ano, em janeiro.

Eu também queria destacar essa questão do fornecimento de dados do WhatsApp. Existe uma matéria muito interessante que está lincada no meu relatório, matéria da *Forbes*, que analisou todas as requisições na Justiça americana que o FBI fez para o WhatsApp, e eles verificaram que tipo de informação o WhatsApp fornecia para o FBI. Basicamente, o que a investigação da *Forbes* mostrou é que o WhatsApp fornece metadados. Ele não fornece nunca, porque ele realmente não tem acesso ao conteúdo das mensagens, mas ele pode fornecer um metadado do tipo: esse celular se conectou à rede do WhatsApp a partir daquele IP, naquela hora, naquele dia - o que você pode mapear para a casa de uma pessoa, para uma cafeteria, o que seja.

Essa metodologia de identificação que eu estou propondo também trata de metadados, ou seja, a gente não estaria pedindo para o WhatsApp dar o conteúdo daquele arquivo; eu só quero saber quem foi a pessoa que enviou aquele arquivo... Desculpe, qual foi o terminal que enviou aquele arquivo. Então, também é um metadado, embora, por ser um tipo de solicitação que me parece inédita, até em nível mundial, porque ela usa um conhecimento de como o WhatsApp funciona, que não é muito difundido, eu acredito que não exista, que essa resposta do WhatsApp não abranja especificamente esse ponto. Então, eu acho que seria um ponto importante para esclarecer, porque permitiria justamente essa colaboração investigativa.

Sobre a questão de diferença entre países e de estar importando esse fenômeno, sim, quer dizer, a gente tem, inclusive, diferenças de legislação entre países, com que o WhatsApp tem tido que lidar. Quer dizer, se a gente tem uma legislação no Brasil que obriga essa guarda de seis meses dos registros, como é que o WhatsApp vai fazer, se um outro país exigir um prazo diferente? Então, há uma diferença legal e há também uma diferença no fenômeno da disseminação das *fake news* no Brasil muito ligado, me parece, ao WhatsApp, por uma questão de que as pessoas no Brasil usam muito o WhatsApp. O SMS, que era a alternativa anterior, era caro, os planos de dados cobravam não sei quantos centavos por cada SMS; entra o WhatsApp, uma opção gratuita que começa a dar muito mais recursos. Então, as pessoas usam maciçamente isso. Isso não é um fenômeno que acontece com essa mesma intensidade em todos os países.

Sobre as *deepfakes* o meu colega já comentou. Eu só faria um adendo de que, pelo que eu já lei, pessoas que trabalham com isso falando, há um custo computacional hoje, para você gerar essa *deepfake*, que, em princípio, é alto, mas você sempre tem que considerar que um custo computacional amanhã não é nada. Então, isso não pode ser considerada uma barreira para que esse recurso seja, cada vez mais, utilizado. Eu acho que vai ser interessante quando a gente começar a ter casos reais de *deepfakes* - é verdade -, começar a ter casos reais de *deepfake* tentando, porque a gente vê muitas demonstrações.

Eu acho que vai ser interessante quando a gente tiver uma propagação real de uma *deepfake* relevante, e a gente vir qual vai ser a resposta da mídia, ou, enfim, qual vai ser a resposta social com relação àquilo e se isso eventualmente pode ter um efeito positivo de criar uma educação maior sobre essa possibilidade. Eu acho que é ainda uma questão em aberto.

O Senador Humberto Costa fez uma pergunta importantíssima sobre as comunidades particulares do WhatsApp, pessoas que não se conhecem. Eu sei que houve, inclusive, na eleição de 2018, uma negativa de um juiz eleitoral, usando esse argumento de que ele não poderia dar uma certa liminar, porque se tratava de uma comunicação privada, particular. E eu tenho a visão de que grupos - e aí eu não colocaria nem pela questão das pessoas não se conhecerem, que isso é um pouco talvez subjetivo - em que você gera um convite público e você publica esse convite nas suas páginas de Facebook, em blogues, na internet; esse é um grupo público na minha visão. Então, o fato de ele estar hospedado no WhatsApp, como um grupo do WhatsApp, eu vejo como uma diferença técnica, mas que não deveria alterar a natureza com que a Justiça vê esse grupo. Isso é minha opinião pessoal, porque, senão, você está se escondendo numa tecnicalidade, porque você coloca um convite público numa página pública, e você pode conseguir uma liminar para tirar essa página pública do ar, se ela cometer algum crime. E aí a pessoa que entra nessa página e que acessa aquele grupo pode cometer crimes à vontade dentro daquele grupo e não há nenhum tipo de responsabilização? Eu, pessoalmente, acho que essa tecnicalidade não deveria definir a natureza público-privada desses grupos - e talvez mais pela questão do convite público, mostrando que é um grupo aberto. Eu não tenho informação desses grupos ligados com o *site* e também não tenho informação sobre o período do *impeachment*.

O Senador Rogério perguntou sobre a identificação do primeiro disparo. Eu queria só destacar que não é exatamente um primeiro disparo de mensagem qualquer, porque - a apresentação fica disponível, não é, Presidente? - a mensagem continua sendo protegida com criptografia fim-a-fim, e quando uma mensagem é repassada, uma mensagem de texto é repassada de um usuário para outro usuário, você não tem nenhum tipo de rastreamento possível. É realmente uma característica ligada ao anexo, quer dizer, ao anexo da mídia. A mídia - vídeo, imagem, áudio e PDF - que você anexa na sua mensagem de WhatsApp recebe um tratamento diferenciado pelo WhatsApp para efeitos até de otimização do desempenho da plataforma, de escalabilidade da plataforma, que gera essa URL, que é um identificador inequívoco daquele material e que é o que poderia ser usado numa investigação. Então, se você tem um primeiro disparo de texto, e esse disparo é repassado, repassado e repassado, eu não tenho nenhuma forma de fazer um rastreamento desse disparo em texto.

Sobre a questão de se tudo fica registrado, se está no equipamento físico, eu, particularmente, acho inviável por um limite talvez legal. Se você tem a cobertura, por exemplo, que o marco civil dá hoje, de que eu posso chegar para um provedor, eu digo assim... Eu juiz, por exemplo. Eu juiz chega para um provedor de conteúdo e fala: "Eu preciso deste registro aqui de acesso, porque isto aqui está no período de seis meses, em que você é obrigado a manter esse registro". Então, o provedor de aplicação vai fornecer aquele registro. Passados os seis meses, o provedor fala: "Eu não tenho mais; eu apaguei". Eu posso até concordar, em tese, com você que eventualmente um registro que ele apagou pode ter ficado num HD físico que está em algum lugar da sede da empresa. Agora, se você for entrar nesse tipo de investigação, você teria que fazer uma busca e apreensão dos computadores da empresa para poder fazer uma perícia. Então, eu acho que isso excede o escopo possível de investigação. Eu acho que o que está previsto no marco legal é uma janela interessante que já foi pensada justamente para esse tipo de situação.

Com isso acho que eu encerro as perguntas.

O SR. PRESIDENTE (Angelo Coronel. PSD - BA) - Eu queria prestar aqui algumas informações. A Senadora Kátia Abreu não se encontra, mas informo a todos os senhores e as senhoras que a Anatel, a partir de janeiro, agora, já disponibiliza um *site* para consulta dos telefones que estão cadastrados no seu CPF. Então, se alguém tem seu CPF, qualquer pessoa, até por maldade, chega lá, faz a habilitação de um *chip*. A partir de janeiro já vai ter esse crivo. E também, a partir de janeiro, a Anatel vai exigir mais rigor na habilitação dos *chips*. Provavelmente, com a presença física da pessoa, munida do CPF ou procuração, para evitar também que laranjas sejam utilizados para fazer essas habilitações.

Então, nada mais havendo a tratar, inclusive, eu queria fazer até essa menção. Nós só vamos encerrar a reunião antecipadamente, porque a nossa Relatora tem um compromisso, vai viajar, pegar avião. Então, em homenagem a ela, boa baiana, nós vamos aqui antecipar. Sei que V. Exas. poderiam questionar os nossos convidados, mas vamos deixar para outra oportunidade. Eles vão disponibilizar este material aqui para as nossas consultas. Sei também que eles vão ficar à disposição para qualquer ligação ou até uma outra vinda aqui, se possível for, para demais esclarecimentos.

Então, nada mais havendo a tratar, agradeço a presença de todos, a presença do Dr. Miguel Freitas, do Dr. Marco Aurélio. Foram muito importantes as apresentações de vocês. Foi de grande valia para esta Comissão. Tenho certeza de que isso vai surtir frutos no futuro.

Então, convido a todos para a próxima reunião, que se realizará no dia 3/12, às 13h, com os seguintes convidados: Natália Leal, representante da Agência Lupa; Thiago Reis, representante do *site* Fato ou Fake, do Portal G1; representante da Associação Brasileira de Imprensa (ABI); representante da Federação Nacional dos Jornalistas (Fenaj).

E, no dia 4/12, acabei de confirmar aqui, agora, a convidada confirmou a presença, a Deputada Joice Hasselmann, também às 13h.

Declaro encerrada a presente reunião.

E vão com Deus!

(Iniciada às 13 horas e 29 minutos, a reunião é encerrada às 15 horas e 36 minutos.)