# RASTREAR O VIRAL?

## RISCOS À PRIVACIDADE NO PROJETO DE LEI "DE COMBATE ÀS FAKE NEWS"

Diagnósticos & Recomendações nº3

JULHO 2020

# RASTREAR O VIRAL?

## RISCOS À PRIVACIDADE NO PROJETO DE LEI "DE COMBATE ÀS FAKE NEWS"

Diagnósticos & Recomendações nº3



### COMO CITAR ESSE DOCUMENTO

InternetLab.
**Rastrear o viral? Riscos à privacidade no projeto de lei "de combate às fake news".**
InternetLab, São Paulo, 2020.


### EQUIPE DO PROJETO

**INTERNET LAB**
Francisco Brito Cruz e Mariana Valente

**EDITOR-GERAL**
André Cabette Fábio

**PROJETO GRÁFICO**
Marina Zilbersztejn

### EQUIPE INSTITUCIONAL

**TECH FELLOW** Alessandra Gomes

**ESTAGIÁRIA DE PESQUISA** Clarice Tavares

**ESTAGIÁRIO DE PESQUISA** Victor Pavarin Tavares

**PESQUISADOR** Enrico Roberto

**PESQUISADORA** Ester Borges

**COORDENADORA DA ÁREA DE INFORMAÇÃO E POLÍTICA** Heloisa Massaro

**ENCARREGADA ADMINISTRATIVA** Laís Denúbila

**COORDENADORA DA ÁREA DE PRIVACIDADE E VIGILÂNCIA** Nathalie Fragoso

**COORDENADOR DE COMUNICAÇÃO** Sérgio Motta

**COORDENADOR DA ÁREA DE LIBERDADE DE EXPRESSÃO** Thiago Oliva

INTERNETLAB
pesquisa em direito e tecnologia

# ÍNDICE

# APRESENTAÇÃO

## O QUE É O INTERNETLAB?

O InternetLab é um centro independente de pesquisa interdisciplinar que produz conhecimento e promove o debate em diferentes áreas que envolvem tecnologia, direito e políticas públicas.

Somos uma entidade sem fins lucrativos baseada em São Paulo, que atua como ponto de articulação entre pesquisadores e representantes dos setores públicos, privado e da sociedade civil. Partimos da ideia de que a formulação de boas políticas públicas depende de diagnósticos mais precisos sobre a relação entre tecnologias da informação e comunicação — como a internet — e os direitos das pessoas.

Veja mais no nosso site: www.internetlab.org.br

## QUAL O OBJETIVO DESTE DOCUMENTO?

Esta é uma mais intervenção do InternetLab para melhoria do debate público democrático e enfrentamento da desinformação na internet. Neste documento, o assunto é o enfrentamento da desinformação a partir da regulação de aplicativos de mensagens privadas, como o WhatsApp.

O debate tem como ponto de partida o projeto da "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet", aprovado no Senado no final de junho de 2020, e conhecido como "PL das Fake News". Dentre outros objetivos, este projeto pretende dar uma resposta ao uso de aplicativos de mensageria privada em campanhas de desinformação ou de ofensas a pessoas e instituições.

Um de seus pontos mais polêmicos é o artigo que determina a guarda obrigatória de registros de encaminhamento de mensagens que acabam se tornando virais, construído em uma tentativa de responsabilizar disseminadores de conteúdo ilegal.

Este ponto determina a coleta, portanto, de dados sobre as mensagens encaminhadas, assim como sobre seus encaminhadores. O nome técnico para esses *dados sobre outros dados* é "metadado". Buscando aprofundamento sobre os impactos e riscos a direitos fundamentais da proposta de retenção de metadados de mensagens prevista no projeto de lei, o InternetLab entrevistou cinco especialistas de áreas diferentes. Vale apontar que, dentre os entrevistados, ninguém defende a proposta do PL.

Não é o objetivo deste documento descrever diferentes posições em debate, mas qualificar as preocupações sobre violações que podem decorrer dessa medida — alinhadas com a trajetória de trabalho de pesquisa do InternetLab sobre a proteção do direito à privacidade frente à vigilância sobre as comunicações eletrônicas.

# PRINCIPAIS PONTOS EM DISCUSSÃO

> O artigo 10 do "PL das Fake News" aprovado no Senado determina a retenção dos registros de encaminhamentos de mensagens, com o objetivo de rastrear sua origem. Isso vale para aplicativos com no mínimo 2 milhões de usuários — como o WhatsApp ou o Telegram.

> Segundo a proposta, estes aplicativos passariam a ser obrigados a reter, por três meses, "registros dos envios de mensagens veiculadas em encaminhamentos em massa".

> O texto define "encaminhamento em massa" como o envio da mesma mensagem para no mínimo 1.000 pessoas. Essas mensagens devem ter sido enviadas inicialmente a grupos e listas por mais de cinco usuários, dentro de um intervalo de até 15 dias.

> Os registros retidos devem incluir a indicação dos usuários que encaminharam a mensagem, o horário dos encaminhamentos e a quantidade de pessoas que a mensagem atingiu.

> Os metadados poderão ser obtidos no curso de uma investigação ou processo criminal a partir de uma ordem judicial.

# PONTOS LEVANTADOS PELOS PESQUISADORES

A pesquisadora e advogada especializada em criptografia **RIANA PFEFFERKORN** afirma: "A exigência de retenção de metadados poderia levar ao fim da criptografia de ponta a ponta".

O historiador especializado em regimes autoritários no Brasil **CARLOS FICO** afirma: "Não duvido das boas intenções dos legisladores, mas me parece claro que a proposta está excessivamente contaminada pelo cenário político relativo a diagnósticos apressados".

A pesquisadora e advogada especializada em direito e tecnologia **JACQUELINE ABREU** afirma: "Criminosos mais sofisticados poderão, por exemplo, simplesmente utilizar-se de estratégias de envio de fora do Brasil, ou usar os limiares indicados como instruções sobre como não serem pegos".

O pesquisador e advogado especializado em direito e tecnologia **AMBER SINHA** diz sobre uma tentativa similar na Índia: "O WhatsApp não verifica dados de nacionalidade, por isso não se sabe como essa medida seria implementada especificamente na Índia".

O advogado constitucionalista e jornalista **GLENN GREENWALD** afirma: "Quanto mais poder damos para as empresas, mais poder damos aos grupos poderosos. O discurso de proteger minorias pode ser o pretexto, mas não seria a forma como esse poder seria utilizado".

# RIANA PFEFFERKORN

Diretora associada de Cibersegurança e Vigilância no Centro para Internet e Sociedade da Universidade de Stanford. No setor privado, Riana trabalhou em litígios envolvendo privacidade online e proteção do consumidor, entre outras áreas. Como pesquisadora, analisa práticas governamentais e legais que influenciam a criptografia ou descriptografia de serviços online.

**"O projeto significa uma grande base de dados com mensagens de todo mundo"**

## [MUDANÇAS NOS APLICATIVOS DE MENSAGENS]

**1 De um ponto de vista técnico, que tipo de mudanças seriam necessárias na forma como aplicativos de mensagem funcionam, para que se adequassem à retenção dos dados ligados ao encaminhamento em massa?**

Eu acredito que é correto dizer que cada mensagem encaminhada precisaria ser retida por um período de pelo menos 15 dias, só por via das dúvidas, para o caso de que fosse enviada por cinco usuários nesse período. Exemplo: eu envio uma mensagem para uma pessoa no dia 1, e depois no dia 14 outras quatro pessoas enviam a mesma mensagem. Isso poderia se encaixar nos termos da lei.

Em tese há um limite: "A obrigatoriedade de guarda prevista neste artigo não se aplica às mensagens que alcançarem quantitativo total inferior a 1.000 (mil) usuários." Mas de que forma o serviço privado de mensagens sabe, no dia 1, se a mensagem chegará a 1001 ou a 999 usuários até o dia 15? Por isso, me parece que o provedor precisaria manter todos os metadados das mensagens.

Além disso — será que o período de retenção de três meses termina três meses depois de a primeira mensagem ter sido enviada? Ou ele termina 14 dias depois, após ter sido enviada por quatro pessoas? Não é nem mesmo uma lei bem escrita.

## 2 [RISCOS À PRIVACIDADE E À SEGURANÇA]

**Essas mudanças podem trazer mais riscos à segurança e à privacidade dos usuários? Em caso positivo, quais são os maiores riscos para aqueles que não estão envolvidos em atividades ilegais ou no compartilhamento de desinformação?**

"Da forma como eu leio, o projeto de lei requer que provedores possam ler os conteúdos de todas as mensagens, e retê-las por três meses [Nota da edição: o projeto de lei não fala, em nenhum momento, sobre retenção de conteúdo das mensagens. Riana explica, na próxima pergunta, como entende que, do ponto de vista técnico, não é possível reter os metadados das mensagens sem "ler" os conteúdos]. Isso significa menos segurança e privacidade para os usuários, porque significaria uma grande base de dados com as mensagens de todo mundo. Ela poderia ser hackeada, ou sofrer algum tipo de violação, apesar das obrigações que a lei estabelece em relação às informações.

Exigir a retenção de mensagens também significa que os provedores não poderiam mais oferecer "features" de "desaparecimento de mensagens" [quando uma mensagem se autodeleta depois de certo período]. Isso também é ruim, porque a efemeridade é um componente importante da privacidade. Você deveria poder dizer algo a alguém sem criar nenhum registro.

Também é uma enorme invasão de privacidade que os provedores sejam forçados pelo governo a guardar (e entregar para a polícia) toda essa informação sobre as conversas de todo mundo: quem está falando com quem, o que foi dito, e quando; quem está em quais grupos, quem mais está nesses grupos; e por aí vai. São informações que os provedores já poderiam rastrear de qualquer forma (por exemplo, com os "social graphs" [gráficos criados pelas redes sociais que mapeiam como os usuários se relacionam entre si] das mídias sociais), mas é assustador quando é o governo que os impele a fazer esse rastreamento, e mantê-lo por um período tão longo.

Além do impacto sobre a segurança da informação e a privacidade dos usuários, essa lei levará à autocensura — o "efeito coercitivo" que a vigilância tem sobre a liberdade de expressão.

A lei diz que pretende respeitar a livre expressão, e que não tem a intenção de ser aplicada contra a "manifestação artística, intelectual ou de conteúdo satírico, religioso, político, ficcional ou literário, ou a qualquer outra forma de manifestação cultural". Apesar disso, usuários no Brasil têm ótimos motivos para suspeitar que autoridades brasileiras abusariam do poder de exigir os registros de suas mensagens privadas, de forma que muitas pessoas provavelmente se distanciarão, por medo, das atividades perfeitamente legais para as quais usam seus serviços privados de mensagens.

## [CRIPTOGRAFIA]

## 3 Você acha que uma regra para retenção de metadados em aplicativos de mensagem poderia impactar a criptografia de ponta a ponta?

Acredito que a exigência de retenção de metadados poderia levar ao fim da criptografia de ponta a ponta. Vamos voltar ao exemplo da questão 1: eu envio uma mensagem a uma pessoa no dia 1, e depois outras quatro pessoas enviam a mesma mensagem no dia 14. Minhas mensagens são criptografadas de ponta a ponta.

De que maneira o provedor poderia saber que as mensagens do dia 1 e do dia 14 são a mesma, a não ser que conseguisse ler o conteúdo? Logo, a única forma de saber qual mensagem pode ser considerada "de encaminhamento em massa" é vendo os conteúdos das mensagens, o que é incompatível com a criptografia de ponta a ponta.

A tecnologia de ponta a ponta é aplicada aos serviços de mensagem em massa para que as pessoas possam se comunicar umas com as outras sem que ninguém as espione. Mas me parece que essa lei forçaria os provedores a espionarem e manterem registros do que todo mundo está dizendo, quem está dizendo e para quem está dizendo. Isso não é compatível com a privacidade das conversas.

Não consigo enxergar de que forma essa lei poderia atingir tanto os objetivos de preservar a privacidade dos usuários e a liberdade de expressão quanto os objetivos de reter e manter a rastreabilidade das mensagens. Me parece que há um conflito direto.

# CARLOS FICO

Professor titular de História do Brasil da UFRJ (Universidade Federal do Rio de Janeiro) e pesquisador do CNPq. Ele desenvolve pesquisas principalmente sobre ditadura militar no Brasil e na Argentina, historiografia brasileira, rebeliões populares no Brasil republicano e história política dos Estados Unidos durante a Guerra Fria.

**"Quando supervalorizamos as chamadas *fake news* não estamos tendo perspectiva histórica"**

## [LIGAÇÕES ENTRE PASSADO E PRESENTE]

### 1 Como a preocupação com "desinformação" ocorreu em outros momentos na história brasileira, e qual foi a resposta estatal?

O que vem imediatamente à mente são, obviamente, as tentativas de censura, que sempre ocorreram de diversas formas na história brasileira, sobretudo nas duas ditaduras (Estado Novo e Ditadura Militar).

Governos autoritários tentaram justificar iniciativas como a censura ou a "Lei de Imprensa" da ditadura com o argumento de proteção da sociedade: proteção da "moral e dos bons costumes" ou para evitar "manchetes chamativas" — como diziam os militares na ditadura.

Há outros exemplos que também poderiam ser lembrados, como o escândalo das "cartas falsas" (1921), o falso "Plano Cohen" (1937) ou a "Carta Brandi" (1955) — todos episódios de informação falsa que tiveram graves consequências políticas.

Mas eu não creio que o cenário atual tenha muito a ver com esses fenômenos do passado. Acho que nos falta um bom diagnóstico do impacto atual da informática na vida contemporânea. O que se vê, hoje, é a expressão popular — muito acentuada pelas redes sociais e pelos aplicativos de mensagens instantâneas — de grandes doses de ressentimento (com o fracasso das políticas de amparo social) contra lideranças em geral — lideranças políticas, lideranças intelectuais, "especialistas"...

Esse ressentimento, como se sabe, não se verifica apenas no Brasil, embora aqui se relacione mais aos problemas da segurança pública, da saúde e outros dessa natureza, diferentemente dos casos de países europeus ou dos EUA (previdência, imigração etc.).

Sabemos que, em outros momentos históricos, esse tipo de ressentimento se expressou não apenas como revolta política *stricto sensu* (manifestações sociais, por exemplo), mas também como zombaria, deboche e/ou rejeição acrimoniosa do establishment. Lembro, por exemplo, da "candidatura" a prefeito do macaco Tião (1988) ou do voto de protesto na rinoceronte "Cacareco" (1959).

Uma das dimensões importantes das redes sociais é a possibilidade de expressão dessa "perversidade lúdica", como eu a chamo. Manifestações hoje lidas como "discurso de ódio" me parecem ter, na verdade, esse conteúdo de condenação de lideranças que não conseguem resolver os problemas da saúde, da segurança, da habitação etc., apesar de sua "empáfia".

Eu também tenho dito que sempre vivemos o risco da "retórica da iminência", quer dizer, a supervalorização do presente, como se a época na qual vivemos fosse a "decisiva", a culminância da história, quando coisas extraordinárias aconteceriam. É um sentimento muito corriqueiro: o historiador Leopold von Ranke dizia, no século XIX (contra a supervalorização do presente), que "todas as épocas estão próximas de Deus".

Ou seja, quando supervalorizamos as chamadas "fake news" não estamos tendo perspectiva histórica, não estamos tendo o devido distanciamento analítico, pois é evidente que esse é um fenômeno passageiro que integra o longo processo de transformações impostas pela informática. Para o historiador do tempo presente, é fundamental ter distanciamento, na medida em que fenômenos, hoje, aparentemente cruciais, poderão ser, no futuro, meras notas de rodapé.

Nós não temos como controlar e "regulamentar" um processo histórico da dimensão do impacto da informática na vida contemporânea: vamos apenas "tateando", porque se trata de fase de transição. Temos, isso sim, a obrigação de compreendê-lo da melhor maneira possível para não cometermos erros muito graves.

Quando a TV, no Brasil, se configurou mais ou menos como ela é hoje, ali pelos anos 1970 (graças à rede de microondas que permitiu transmissão nacional online), agentes de informações da ditadura pretenderam enquadrá-la porque a TV, segundo eles, seria uma "magnífica máquina de educação popular". Claro que não conseguiram. A TV teve sempre muita influência para o bem e para o mal? Com certeza. Mas o processo de sua consolidação (e de seu atual crescente descrédito) não pôde ser regulamentado.

## [PARALELOS]

## 2 Como um historiador de nosso passado autoritário, de que forma você enxerga a proposta de "rastreabilidade" de mensagens, articulada no PL das Fake News, para posteriores investigações sobre "notícias falsas"?

Eu li o projeto e fiquei muito impressionado com duas coisas: a falta de precisão e o português ruim. A falta de precisão é típica das leis ruins (bem, o português ruim também...). Não duvido das boas intenções dos legisladores, mas me parece claro que a

proposta está excessivamente contaminada pelo cenário político relativo a diagnósticos apressados (fake news seriam responsáveis por eleições de governantes de extrema direita e/ou pela disseminação e aceitação de comportamentos condenáveis).

Como disse na resposta anterior, carecemos de diagnóstico preciso. Não quero fazer comparações injustas, mas lembro das leis de segurança nacional (a última, infelizmente, ainda em vigor): todas eram imprecisas e mal redigidas. Isso gerava problemas até para os insuspeitos ministros do Superior Tribunal Militar (quando julgavam com base nessas leis), que criticavam a falta de clareza dos crimes nelas previstos.

Hoje vemos muitas pessoas recorrendo à Lei de Segurança Nacional para incriminar o "seu" adversário político: é boa para os "outros"; para mim é um "entulho autoritário".

Recentemente, fui convidado pela Câmara dos Deputados para opinar sobre projeto que define como crime a "apologia da ditadura". Creio que decepcionei os parlamentares de esquerda que esperavam minha adesão: na verdade, penso que todos têm o direito de pensar e dizer o que quiserem. Se disso decorrer difamação ou calúnia, já temos legislação adequada. Não se pode condenar ninguém por suas convicções — mesmo que elas nos pareçam tolas ou erradas —, mas pelo que alguém concretamente fez ou faz contra a lei.

Não sou especialista em legislação ou em direito, mas a proposta me parece repleta de imprecisões e de possibilidades de uso indevido de dados, inclusive de metadados, que não deveriam ficar sob o escrutínio de empresas que gerenciam aplicativos de mensagens ou outros (redes sociais).

Não tenho dúvida de que esse projeto deveria ser mais bem discutido (e, se possível, abandonado). Aprovado como está, não contribuirá para a consolidação da democracia. Lembro-me de que um inquérito sobre fake news já está em curso sem a necessidade de uma nova lei.

## 3 [OLHAR PARA O PASSADO PARA PENSAR O FUTURO]

**Pensando em nossa história e de nossas instituições de aplicação da Justiça, quais você acha que poderiam ser as consequências da guarda de dados para investigações posteriores?**

Tenho a impressão de que o projeto, tal como está, permite muitos questionamentos sobre sua constitucionalidade, de modo que há a possibilidade de estarmos discutindo algo irrelevante e que será superado — como frequentemente ocorre em cenários de crises políticas. Não podemos esquecer, ademais, de que o projeto contém alguma dose de inviabilidade.

# JACQUELINE ABREU

Doutoranda em direito na Faculdade de Direito da Universidade de São Paulo, advogada e membro da Comissão de Juristas da Câmara dos Deputados para proteção de dados e segurança pública. Jacqueline tem como foco de pesquisa direito e tecnologia, e direitos fundamentais.

**"A proposta intervém nos direitos ao sigilo das comunicações e à proteção de dados"**

## [DIREITOS FUNDAMENTAIS]

**1 Como a retenção de dados para posterior investigação se relaciona com direitos fundamentais? A proposta pode trazer conflitos com a Constituição?**

O artigo 10, na forma aprovada no Senado, impõe a serviços de mensageria privada um dever de guarda preventiva de "registros de envio de mensagens veiculadas em encaminhamentos em massa". Encaixam-se nessa definição as mensagens que (i) tenham sido enviadas a grupos/listas/assemelhados (ii) por mais de cinco pessoas (iii) dentro de 15 dias e que (iv) tenham alcançado ao menos 1000 pessoas. Isso seria feito para o caso em que registros de envio dessas mensagens venham a se tornar úteis para investigações criminais.

Esse é mais um tipo de norma de retenção de dados porque, grande parte das vezes, dados sobre quem enviou mensagens ou que mensagens a quantas pessoas em algum período de tempo não são guardados por empresas para suas operações. Guardas de dados sempre representam custos e, quando não há necessidade de uso dessas informações, elas são descartadas.

Impõe-se a guarda, portanto, para uma finalidade estranha à original e comercial do serviço. Essa guarda é preventiva — para o caso de vir a se tornar útil para uma investigação.

Na Europa, esse tipo de medida já foi diversas vezes questionado pela sua incompatibilidade com o direito à autodeterminação informacional e ao sigilo de comunicações, mais fundamentalmente por colocar todas as pessoas, indistintamente e sem necessidade de vínculo a atividade suspeita, sob monitoramento. E também por não atender concretamente a critérios de proporcionalidade ao impor o dever de coleta e retenção massiva de dados pessoais.

Nós temos normas de retenção obrigatória hoje em dia no Brasil, no contexto de telecomunicações — para registros telefônicos e também para informações de conexão à internet e acesso a aplicações. Essas normas já são objeto de preocupação.

A novidade dessa proposta (art. 10 do PL) está em dar um passo além, a meu ver: ela cria uma infraestrutura de monitoramento que está necessariamente vinculado ao conteúdo de mensagens.

Para ser capaz de reter metadados sobre uma mensagem (no caso, informações sobre usuário que enviou, data e hora) e verificar se ela atende aos limiares fixados, é preciso necessariamente etiquetar, de algum modo, uma mensagem e vinculá-la aos tais registros de envio.

Por exemplo, para saber se uma mesma mensagem foi enviada em massa, eu preciso ser capaz de atribuir, desde o início, uma informação única — um tipo de identificação — sobre o teor da mensagem. Essa informação deve me permitir contabilizar se mais de 5 pessoas enviaram a mensagem a grupos, e depois verificar se ela alcançou 1.000 pessoas dentro de 15 dias. Como, em um prazo de 15 dias, eu não sei que mensagens vão atender a tais características, deverá haver retenção de registros de toda e qualquer mensagem enviada em grupos/listas, vinculados aos conteúdos, nesse período. 100%.

Nesse contexto, sim, a proposta suscita preocupação por intervir nos direitos ao sigilo das comunicações e à proteção de dados pessoais, o que baseia o entendimento de que há conflito com a Constituição Federal: coletam-se dados em excesso, inclusive vinculados a conteúdo de comunicações — quem escreveu o quê, onde, quando.

Não deixa também de caracterizar uma interferência sobre a liberdade empresarial. A empresa teria que adaptar seu sistema de forma que lhe parece inconsistente com seu compromisso com os usuários.

Um argumento em defesa que com frequência se faz é que não deve haver proteção de sigilo/privacidade sobre uma mensagem/comunicação que ganhou escala — e que deixaria de ser *privada* e se tornaria pública. Entendo o ponto, mas ele olha só para um aspecto externo; ele não responde à preocupação sobre a infraestrutura de coleta e monitoramento preventivo está sendo imposta — e os riscos daí decorrentes.

## 2 [PROBLEMAS E ABUSOS NA APLICAÇÃO]

**Você pesquisa como as autoridades de investigação e o Judiciário requerem dados de usuários de internet como provas em inquéritos e processos. Qual seria o impacto da proposta de "rastreabilidade" do PL das Fake News na prática, inclusive para processos que não têm a ver com desinformação?**

Decisões judiciais mal fundamentadas, que não analisam preenchimento de requisitos legais, que se excedem aos limites e hipóteses previstas e a noções de razoabilidade são problemas associados a certos pedidos de fornecimentos de dados e quebras de sigilo. A suposição cultivada de que o requisito formal — existir uma ordem judicial mandando ou autorizando X — é suficiente, sem atenção à observância de critérios materiais e substantivos, infelizmente, não ajuda. É difícil, portanto, achar que algo assim não aconteceria neste caso — que não haveria diversas releituras desse dispositivo e usos secundários da infraestrutura criada para ir muito além daquilo previsto.

Por exemplo, vale notar que o dispositivo fala em "conteúdo ilícito" — e não em "conteúdo ilícito vinculado a campanhas de desinformação". Há muita coisa que autoridades consideram ser conteúdo ilícito, mas que outros defenderiam como liberdade de expressão legítima.

Se uma notícia com uma denúncia ou um vídeo de humor mais ousado for veiculada em uma mensagem que se encaixa na definição da lei, e seus conteúdos forem considerados ilícitos, isso seria suficiente para que pessoas que encaminharam a mensagem se tornassem alvo de investigação, de modo questionável.

É por isso que, além da preocupação com a privacidade, há também uma preocupação com efeitos inibidores da própria liberdade de expressão: medo de encaminhar certa mensagem em um grupo/lista porque sabe-se lá se alguém não vai considerar o teor ilícito.

E a entrega desses registros, vale lembrar, é irreversível.

Ainda que se pudesse cogitar algo assim, o dispositivo não traz nenhum parâmetro sobre o que justificaria o pedido de fornecimento dos registros de encaminhamento. Qual é o atributo técnico necessário para que o provedor possa fazer a localização inequívoca do material e fornecimento dos registros pertinentes?

O dispositivo serve ainda para criar falsas expectativas — de que sempre vai ser possível rastrear a origem e, se não for, é porque o provedor está dificultando/não está atendendo à lei. Isso também tende a gerar um problema de ordem prática, e muito atrito no cumprimento de ordens, o que alimenta um cenário de insegurança jurídica pouco atraente a operações no Brasil.

## 3 [NECESSÁRIA E PROPORCIONAL]

### Como você avalia a necessidade e a proporcionalidade desta proposta de retenção de dados do PL das Fake News? Como ela posicionaria o Brasil internacionalmente?

O objetivo da proposta é rastrear a origem de mensagens com conteúdos ilícitos — notadamente fake news — e assim responsabilizar os criadores. Hoje, em muitas ocasiões, isso é impossível. Infelizmente, não podemos presumir que esse objetivo será alcançado. Criminosos mais sofisticados poderão, por exemplo, simplesmente utilizar-se de estratégias de envio de fora do Brasil, ou usar os limiares indicados como instruções sobre como não serem pegos (deixar de mandar X mensagens mais de 5 vezes em 15 dias, passar a mandá-las por "copia e cola", ou então fazer pequenas alterações no conteúdo a cada envio, por exemplo).

Acho, portanto, que a pergunta — e o problema — é anterior à necessidade e à proporcionalidade. A pergunta é: isso é adequado àquilo que se pretende? Se não for, ou se for pegar no máximo um grupo não relevante de produtores de desinformação, não entendo ser possível justificar a criação dessa infraestrutura de monitoramento preventivo, que interfere em direitos fundamentais.

# AMBER SINHA

Advogado indiano focado no impacto da tecnologia, da internet e na forma como interagem com a lei. Sinha trabalha para o Centro de Internet e Sociedade indiano, onde chefia programas sobre privacidade, big data, cibersegurança e inteligência artificial.

**"Os requerimentos para rastreamento ignoram as melhores práticas de privacidade"**

## [O CASO INDIANO]

**1 Você pode descrever a proposta de retenção e rastreabilidade de dados na Índia, o que a motivou e qual foi a resposta a ela?**

Em 2018, uma petição foi apresentada à Alta Corte de Madras [capital do estado de Tâmil Nadul, no sul da Índia], buscando determinar a obrigação de linkar e-mails e contas de mídias sociais a alguma identificação mantida pelo governo, como o Aadhaar [um número de identificação único, que pode ser obtido por cidadãos indianos ou pessoas com passaportes que residam na Índia].

Os responsáveis pela petição haviam sido vítimas de abusos on-line. Durante o processo, a corte restringiu as deliberações a uma questão: sobre se plataformas como o WhatsApp, que fornecem serviços criptografados, deveriam criar métodos que permitissem rastrear as mensagens. A corte consultou o professor Kamakoti, que leciona no Instituto Indiano de Tecnologia de Madras, e que também é membro do comitê consultivo do primeiro ministro.

Ele desenvolveu uma proposta, que avaliava que a rastreabilidade era, de fato, possível para o WhatsApp. Mas ela era questionada por outros especialistas, assim como pelo próprio WhatsApp. Posteriormente, esse e todos os outros casos relacionados às questões de responsabilização de intermediários foram transferidos para a Suprema Corte da Índia.

Este debate sobre políticas públicas vem fervilhando na Índia desde 2018. Em dezembro daquele ano, o Ministério de Eletrônica e Tecnologia da Informação divulgou um conjunto de esboços de regras que incluía uma cláusula com requerimentos de rastreabilidade. Esse esboço afirma que "o intermediário deverá permitir a rastreabilidade do responsável pela origem de uma informação em sua plataforma, o que poderá ser requerido pelas agências

governamentais que forem legalmente autorizadas para tanto". Houve uma resposta contrária a esse requerimento, tanto por parte da indústria quanto por parte da sociedade civil.

No decorrer de 2017 e 2018, houve vários casos de linchamentos, nos quais vídeos que circularam pelo WhatsApp tiveram um papel. Outras questões, como o escândalo Pegasus [um spyware desenvolvido por uma empresa israelense de tecnologia que foi usado para interceptar mensagens do WhatsApp de jornalistas e autoridades] de espionagem, deram mais munição à decisão do governo de abordar questões de rastreabilidade. Atualmente, aguardam-se tanto decisões da Suprema Corte quanto do Ministério de Eletrônica e Tecnologia da Informação.

## [RISCOS À PRIVACIDADE E À SEGURANÇA]

### Quais foram os principais problemas com as propostas?

As regras propostas levantaram diversas questões:

**1.** As propostas dizem que intermediários deveriam viabilizar o rastreamento, de acordo com o que poderia ser requerido por agências governamentais. Não havia clareza sobre se todos os intermediários precisariam realizar arranjos para que ocorresse algum "rastreamento" por padrão, ou se qualquer esforço de "rastreamento" só poderia ocorrer em reação a requisições específicas do governo.

**2.** As sugestões não levam em consideração desafios técnicos. Por exemplo, o fato de que provedores de internet que transmitem tráfego criptografado de um usuário para um serviço não têm acesso aos seus conteúdos, ou a informação granular (como o recipiente final de um conteúdo quando o usuário se comunica por meio de um intermediário).

**3.** Os requerimentos para rastreamento ignoram as melhores práticas de privacidade. É necessário que o design técnico de aplicativos e arquitetura da informação sejam pensados de forma a reduzir a quantidade de informação à qual os atores terão acesso. Esse é um princípio reconhecido pela Lei de Proteção Pessoal de Dados de 2019.

Ainda não está claro como os requerimentos de rastreabilidade serão abordados nas regras.

## [LIÇÕES APRENDIDAS]

### Quais são as principais lições da discussão sobre "rastreabilidade" para a questão da regulação de serviços de mensagem instantâneas, e para o combate à desinformação nessas plataformas?

Seria útil considerar riscos e benefícios da discussão técnica sobre rastreabilidade na Índia. As recomendações técnicas do professor Kamakoti consideram duas abordagens. A primeira abordagem envolve a criação de um originador de informação para cada envio de mensagem de ponta a ponta por meio de um serviço.

Esse originador de informação é adicionado na forma de metadados criptografados à mensagem, e acompanha todas as instâncias do encaminhamento. A segunda abordagem consiste em fazer com que o par da chave da informação criptografada do originador seja guardado pelo provedor do serviço. Essa chave poderá ser usada caso as agências legais requeiram informações. Essencialmente, isso significa a criação de uma backdoor [forma de obter acesso a dados criptografados].

Houve discussões sobre diversas dificuldades técnicas relativas a essas duas abordagens, incluindo o fato de que o WhatsApp não verifica dados de nacionalidade, por isso não se sabe como essa medida seria implementada especificamente na Índia. As implicações de privacidade para tais medidas são extremamente significativas.

# GLENN GREENWALD

**Jornalista, advogado e fundador do site The Intercept. Foi responsável por reportagens sobre documentos vazados por Edward Snowden que revelaram como funciona o sistema de coleta de dados pessoais e vigilância do governo americano sobre seus cidadãos.**

**"Quando o governo tem a informação nas mãos, o risco é muito grande"**

**[PROPOSTA E PRÁTICA]**

**1 Como você vê a proposta de guardar metadados de serviços de mensageria para tentar impedir a propagação de fake news, do ponto de vista de sua efetividade?**

Para mim, sempre tem dois lados em todas as propostas desse tipo. Quando a internet começou, uma das maiores inovações da história humana, ela deu poder de organização, disseminação de informação, comunicação, para pessoas que nunca tinham tido. Sem necessidade de um jornal, uma rede de televisão.

O ponto sempre foi que a internet seria completamente livre. O governo ou empresas não poderiam controlá-la. Então, qualquer tentativa de limitar o poder da internet tem um potencial muito perigoso para mim, porque que pode reduzir, eliminar, controlar o poder da internet de liberar e empoderar pessoas, liberar a humanidade.

Eu entendo, obviamente, o raciocínio por trás de diminuir o número de mensagens que podemos enviar ao mesmo tempo no WhatsApp: tentar impedir a propagação de fake news. Mas essa limitação também vai impedir pessoas que estão tentando se organizar e não têm acesso à Rede Globo, à Folha de São Paulo ou a outros amigos poderosos.

De repente, o WhatsApp ou outros aplicativos que tinham esse potencial não teriam mais. Então, tem dois lados. Um lado bom, que é impedir fake news, e outro, que é limitar a independência. Para mim, a solução é pior do que o problema.

Além disso, a aplicação de uma lei como essa não seria efetiva. É muito fácil evitar essas limitações. Além do mais, Facebook, Google ou Twitter não querem essa responsabilidade. Nunca quiseram controlar o conteúdo, ou a forma como ele é usado. É muito melhor para as empresas não terem essa responsabilidade

Por exemplo, no caso de Vivo, Tim, Net ou Oi, posso ligar para 200 pessoas, fazer uma conferência, e organizar um protesto nazista, racista, qualquer coisa que eu quiser.

E ninguém espera que a Oi ou a Vivo cortem meu serviço. Porque o argumento é que são plataformas neutras, que simplesmente ligam as pessoas, sem responsabilidade de monitorar como o serviço é utilizado.

Esse é o modelo que Google, Facebook e Twitter queriam. Eles começaram a tentar controlar e limitar a forma como seus serviços são utilizados só porque a sociedade exigia isso. Mas, obviamente, não querem limitar o uso do serviço, querem ampliar.

Por isso, mesmo que se criasse uma tecnologia que fosse eficaz, por qualquer motivo, contra discurso de ódio, o Facebook não aplicaria de forma genuína, faria para mostrar que está fazendo. Vai fazer só para agradar a sociedade e dizer "estamos tentando".

Sempre vai ter uma solução tecnológica para evitar essa tentativa de controle. Dá para usar contas anônimas, ferramentas para esconder o local, como o Tor [versão do navegador Firefox focada em manter a identidade do usuário secreta], e muitas outras. Tanto os usuários quanto o Facebook teriam formas de burlar, mesmo se o Facebook tivesse motivos para querer limitar a si mesmo.

O único resultado é que o Facebook teria mais poder para censurar, mas [guardar metadados] não ajudaria com os problemas. Às vezes, ouço pessoas falando sobre Facebook, Twitter, Google, quase como governos benevolentes, que querem ajudar e melhorar a sociedade. Por isso, precisamos que interfiram mais no nosso discurso, no debate, porque vão proteger marginalizados e suprimir discurso negativo.

Mas não tem como as pessoas pensarem sobre empresas grandes dessa forma. O objetivo da empresa grande é lucrar, esse é o compromisso legal, é o propósito, gerar lucro para os donos das empresas. Essas empresas maiores sempre vão agir pelos poderosos, contra os marginalizados. Tem um exemplo muito claro para mim. No final de 2017, fiz reportagens mostrando que o governo de Israel e autoridades da Palestina vinham pedindo que o Facebook derrubasse páginas de pessoas, com o argumento de que incitavam violência, terrorismo.

Em 90% dos casos, o Facebook aceitava os pedidos de Israel contra jornalistas, ativistas grupos em defesa dos palestinos. Porque Israel é muito poderoso no negócio de tecnologia. Os palestinos são pobres, não têm poder nenhum, seus pedidos nunca são aceitos. Por isso, tem muita censura contra os palestinos, não necessariamente porque o Facebook está do lado de Israel, mas porque quer lucrar, e defende as facções mais poderosas.

Quanto mais poder damos para as empresas, mais poder damos aos grupos poderosos. O discurso de proteger minorias pode ser o pretexto, mas não seria a forma como esse poder seria utilizado.

## [METADADOS E PRIVACIDADE]

## 2 Uma das justificativas que têm sido usadas a favor dessas medidas de retenção de metadados é que o conteúdo das informações ficaria preservado, e não haveria violação da privacidade dos cidadãos. Isso remete às revelações feitas por Edward Snowden sobre a vigilância estatal nos Estados Unidos. Quais os riscos envolvidos na guarda de metadados?

Muitas vezes, as pessoas acham que o compartilhamento de metadados não traz riscos, porque não significa o governo ou autoridades invadindo o conteúdo da comunicação.

Mas, na verdade, o metadado mostra mais sobre a sua vida do que o conteúdo. Por exemplo, se uma mulher quer abortar e liga para uma clínica de aborto, você não precisa saber o que ela disse para obter uma informação sobre ela. Se alguém tem HIV e liga para um médico buscando tratamento, isso pode ser o suficiente para saber que a pessoa tem o vírus.

Se você liga para uma mulher que não é sua esposa todo dia às 2 h e fala com ela por uma hora, não é preciso saber o conteúdo da comunicação para revelar o que você está fazendo. O metadado mostra mais do que o conteúdo da sua comunicação, porque mostra quem são seus amigos, as pessoas com quem está trabalhando, seu ativismo, com quem está falando. Pode servir para criar uma ideia muito forte e profunda sobre quem você é, o que faz, por qual motivo.

É uma invasão muito profunda, quando o governo sabe com quem você fala, onde está na internet, para quem manda mensagens, mesmo sem saber o conteúdo. Muitos especialistas acreditam que dá para saber mais de uma pessoa com seus metadados do que com o conteúdo de suas mensagens.

Pode haver algum tipo de proteção. Por exemplo, depois das revelações feitas pelo Snowden, os Estados Unidos criaram proteções novas para a privacidade. O governo tem um órgão que monitora ligações das pessoas estrangeiras. Sob a nova lei, o governo não pode identificar a pessoa com quem o estrangeiro se comunica, tem que esconder a identidade. Para identificar, é preciso um pedido legal.

Mas medidas de proteção como essas dependem da da força das instituições para obedecê-las. Quando o governo tem a informação nas mãos, o risco é muito grande.

## [DADOS E JUSTIÇA BRASILEIRA]

## 3 Você vê questões específicas no sistema de Justiça brasileiro que devem ser consideradas quando pensamos nessas propostas?

Eu não tenho opiniões muito fortes sobre isso. Teria que saber o que o governo teria que mostrar para um tribunal para obter as informações.

Mas posso falar do papel dos juízes nos Estados Unidos. Para descobrir com quem um cidadão se comunica, ou o que o metadado mostra sobre o cidadão, com quem está falando, o governo tem que ir a um tribunal. É um processo secreto, o alvo não vai saber, obviamente.

O governo vai para a Justiça, e tem que mostrar que é algo sério, de segurança nacional, um crime grave. Ele diz: "precisamos obter essa informação ou talvez um ataque terrorista, um crime grave seja cometido". Qual é a motivação do juiz? Ele pensa que se recusar o pedido e o ataque terrorista acontecer, ou um crime grave for cometido, o governo vai culpá-lo. Vai dizer: "tentamos impedir o ataque, mas o juiz disse que não provamos a necessidade de obtera informação. Então o sangue está nas mãos do juiz".

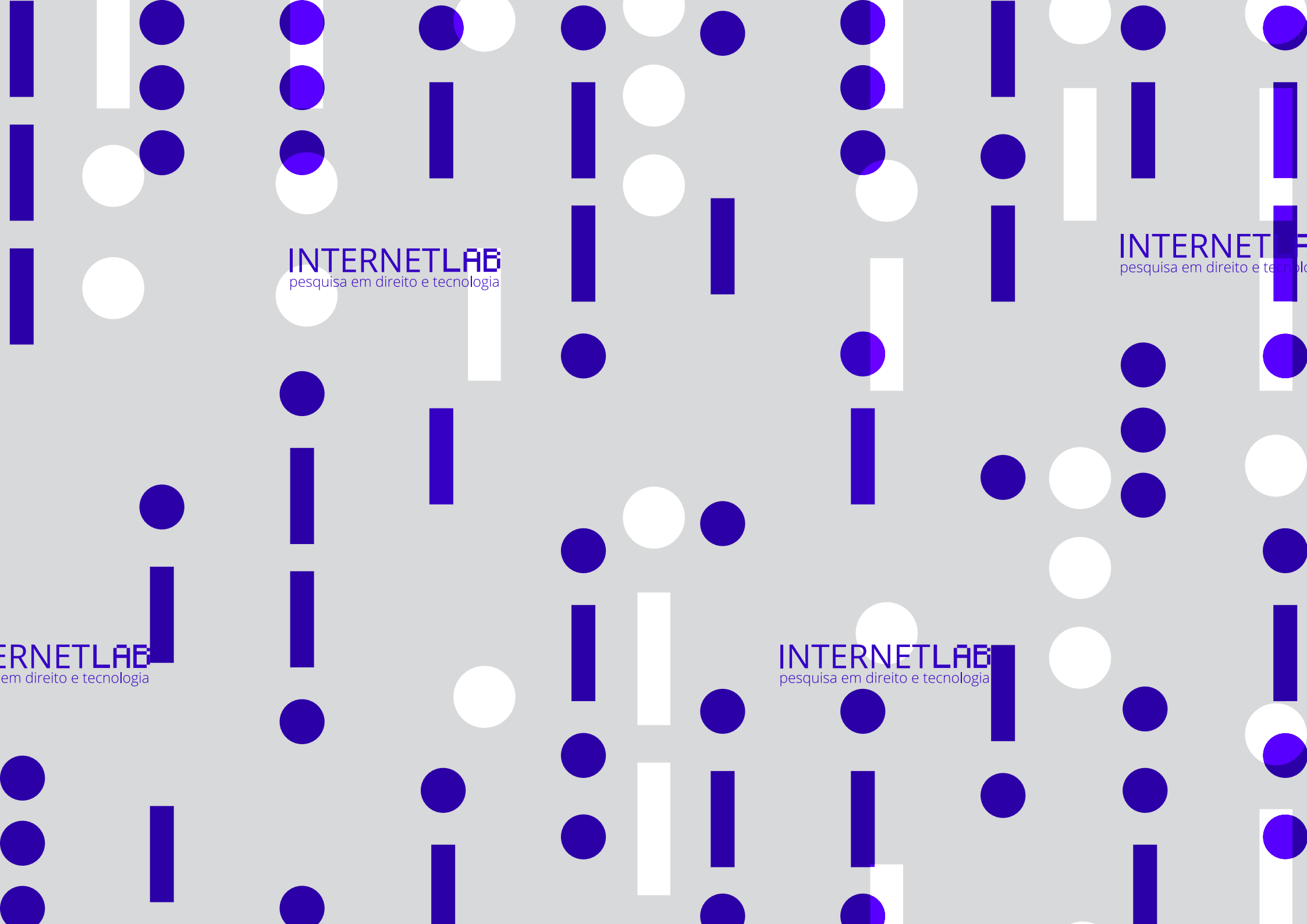
Mas se o juiz aceitar o pedido não tem nenhuma consequência para ele. Quase sempre o juiz aceita o pedido do governo, porque há um incentivo institucional. Esse processo judicial é uma ilusão de proteção. Quase nunca impede que o governo faça o que quiser. É só um processo, e é muito fácil o governo ganhar.

No Brasil, poderia acontecer a mesma coisa. A Polícia Federal, a Abin, a autoridade que quiser a informação vai pedi-la ao juiz, que não vai ter capacidade para saber o que é verdade ou não, e vai ter um incentivo para atender ao pedido do governo.

Além do mais, tenho muitas dúvidas sobre a capacidade de qualquer instituição, governo, empresa, Judiciário, de julgar o que é verdade ou falso, o que é valido para combater discurso de ódio. Porque isso muda o tempo todo.

Entre fevereiro e março, quase quatro meses atrás, a Organização Mundial de Saúde dizia que não era necessário usar máscara contra o coronavírus. Mais ainda, dizia que era perigoso, que a máscara podia aumentar o risco de receber ou transmitir o vírus. Qualquer pessoa que dissesse no YouTube, em fevereiro, que era preciso usar a máscara poderia ser acusada de espalhar fake news, porque ela ia contra o consenso dos cientistas.

Dois meses depois, tudo mudou, agora a máscara é obrigatória, e qualquer pessoa que disser para não usar pode ser acusada de espalhar fake news. É isso que me preocupa muito, dar a uma instituição o poder de dizer o que é falso ou o que é verdade. Não confio em nenhuma instituição para dizer isso.


INTERNETLAB
pesquisa em direito e tecnologia
INTERNETLAB
pesquisa em direito e tecnologia
INTERNETLAB
pesquisa em direito e tecnologia