CÂMARA DOS DEPUTADOS

DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

3ª SESSÃO LEGISLATIVA ORDINÁRIA DA 56ª LEGISLATURA

Grupo de Trabalho (GTNET) destinado a analisar e elaborar parecer ao Projeto de Lei n. 2.630, de 2020 e apensados, que visa ao aperfeiçoamento da legislação Brasileira referente à Liberdade, Responsabilidade e Transparência na Internet (AUDIÊNCIA PÚBLICA EXTRAORDINÁRIA (VIRTUAL))

Em 24 de Agosto de 2021
(Terça-Feira)

Às 9 horas

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Declaro aberta a 8ª Reunião Extraordinária do Grupo de Trabalho de Aperfeiçoamento da Legislação Brasileira na Internet.

Encontra-se à disposição na página do Grupo de Trabalho na Internet a ata da 7ª Reunião Extraordinária. Fica dispensada a sua leitura, nos termos do Ato da Mesa nº 123, de 2020.

Não havendo quem queira retificar a ata, coloco-a em votação.

Os Deputados que a aprovam permaneçam como se encontram. *(Pausa.) (Pausa.)*

Aprovada.

Informo que a Deputada Lídice da Mata enviou escusas pela ausência à reunião de 19 de agosto de 2021 deste Grupo de Trabalho.

Ordem do dia.

A Ordem do Dia de hoje prevê a realização de audiência pública sobre o tema *Como Identificar Agentes Maliciosos Sem Ferir a Proteção de Dados?* A audiência foi convocada atendendo aos Requerimentos nºs 5, 7, 8 e 9, de 2021, respectivamente da Sra. Deputada Natália Bonavides, do Sr. Deputado Rui Falcão, da Sra. Deputada Lídice da Mata e do Sr. Deputado Orlando Silva, o nosso Relator.

Participarão por videoconferência os seguintes palestrantes: Danilo Doneda, professor do Instituto Brasiliense de Direito Público — IDP; Jaqueline Abreu, pesquisadora e membro da Comissão de Juristas de Proteção de Dados Pessoais — PDP; Miriam Wimmer, Diretora da Autoridade Nacional de Proteção de Dados — ANPD; Bruna Martins dos Santos, representante do Data Privacy Brasil Research; Samara Castro, membro do Instituto Nacional de Proteção de Dados — INPD e Vice-Presidente da Comissão de Privacidade e Proteção de Dados e Privacidade da OAB do Rio de Janeiro; e João Brant, Diretor do Instituto Cultura e Democracia.

Para melhor andamento dos trabalhos, eu esclareço que adotaremos os procedimentos que se seguem. O tempo concedido a cada palestrante será de 10 minutos, não podendo haver apartes. Os Deputados interessados em interpelar os palestrantes deverão inscrever-se previamente pelo aplicativo Infoleg, em lista específica. As perguntas serão feitas ao final das palestras e deverão restringir-se ao assunto das exposições, formuladas no prazo de 3 minutos. Os palestrantes terão 3 minutos para responder às perguntas e para as considerações finais.

A reunião está sendo gravada e transmitida ao vivo pela Internet, e todo o conteúdo permanecerá disponível na página da Comissão e poderá ser utilizado pelos serviços de comunicação da Câmara, na sua íntegra ou em parte, para produção de reportagens, documentários e afins.

Feitos esses esclarecimentos, daremos início à nossa audiência.

Com muito entusiasmo, eu passo a palavra para o Dr. Danilo Doneda, professor do Instituto Brasiliense de Direito Público — IDP.

O SR. DANILO DONEDA - Bom dia.

Muito obrigado, Deputada Bruna Furlan. É um prazer participar desta audiência do Grupo de Trabalho de Aperfeiçoamento da Legislação Brasileira sobre Internet.

Congratulo particularmente a Deputada Bruna Furlan, que preside esta reunião, recordando o seu trabalho fenomenal na Comissão Especial que avaliou e aprovou, por unanimidade, a LGPD — Lei Geral de Proteção de Dados. É um prazer estar ao lado dos colegas, muitos conhecidos com relação ao tema, como a Jaqueline Abreu, a Miriam Wimmer, o Bruno Martins dos Santos, a Samara Castro e o João Brant.

O tema da LGPD, que a Deputada Bruna Furlan conhece com bastante detalhamento e precisão, é justamente o contraponto e a consideração necessária que vamos fazer nesta audiência, em relação a métodos e propostas que vêm sendo veiculados e considerados para o combate às *fake news*, à desinformação de uma forma geral.

É evidente que não preciso enfatizar o quanto é necessário esse trabalho de combate, esse trabalho de enquadramento, que passa pela definição do conceito de *fake news*, como ele se caracteriza e quais os mecanismos ideais para combatê-lo. O que eu vou fazer agora é justamente procurar lançar um pouco de luz sobre o papel de dados pessoais e propriamente da LGPD e do direito fundamental à proteção de dados no esquadramento de metodologias para esse combate.

A Lei Geral de Proteção de Dados — LGPD não é, em si, um divisor de águas, mas, acima de tudo, o símbolo de um novo pacto social que já se verificava antes dela, que reconhece a importância fundamental dos dados pessoais para a sociedade nos dias de hoje, para o cidadão que se identifica e que tem acesso a serviços públicos e privados e a relações de trabalho, pessoais e tantas outras somente através dos seus dados, quanto mais agora, em momento de pandemia. Também é um pacto engendrado por atores do setor produtivo e do setor público, que utilizam dados pessoais com cada vez mais desenvoltura, o que proporciona ganhos nas suas atividades e também um desenvolvimento social e econômico que não deve ser, de forma alguma, deixado de lado.

Agora, é claro que esse pacto reconhece, mais que tudo, a necessidade de que dados pessoais não sejam tratados como elementos secundários em qualquer tipo de transação, em qualquer tipo de esquema e ecossistema que os utilize. É necessário que os dados sejam tratados sob os princípios da transparência, que se considere a legitimidade do seu uso, que se coloquem controles para o cidadão sobre o seu uso e que aqueles que vão se utilizar de dados pessoais sejam criativos e proporcionem elementos para que esses direitos sejam colocados igualmente.

Para que isso seja possível, foi necessário desenvolver métodos regulatórios novos. Foi a LGPD justamente a ponta de lança dessa tendência, mas também temos a posição de um sistema administrativo de tutela, representado aqui inclusive pelo Dra. Miriam Wimmer, ilustre Diretora da ANPD. Em outras dimensões, também vemos uma preocupação muito grande de cidadãos e membros de empresas e órgãos em se adequaram à lei.

As soluções para se garantir a legitimidade desse pacto social passam também pela posição de soluções técnicas. A tecnologia tem papel essencial na criação de incentivos e de direcionamentos para que o cidadão possa ter seus dados utilizados de forma mais escorreita e transparente, com controle. A arquitetura de plataformas, a arquitetura — vamos direto ao ponto, porque temos pouco tempo — de sistemas e mensagística, por exemplo, é fundamental para que possamos reconhecer, nesses sistemas, elementos que garantam a efetividade e a presença dos princípios da lei e da consolidação desse pacto.

O urbanista Lewis Mumford falava que a arquitetura faz o homem e o homem faz a arquitetura. Este é um caminho de retroalimentação: nos serviços e produtos que nós concedemos, devemos deixar patentes as nossas opções também em termos de estruturas que legitimem o exercício de direitos. É isso, aliás, que a LGPD traz quando incentiva a chamada "privacidade na concepção", a privacidade por *design*.

Vou direto ao projeto lei em discussão aqui, o PL 2.630/20. Eu acredito que há alguns problemas referentes a isso, principalmente à ideia da rastreabilidade. Eu não vou entrar em detalhes, mas me parece que já foi conversado, de forma extenuante, que a LGPD não é compatível, na forma como é proposta, com a ideia da proteção de dados, porque ela mina um elemento técnico que procura garantir o direito à privacidade. Ela mina a criptografia de ponta a ponta, como já foi demonstrado em falas desta Comissão e em outros fóruns.

Não é possível uma rastreabilidade massificada, que inclusive coloca cidadãos potencialmente sob a mira da rastreabilidade, da verificação disso tudo, sem diminuir a solidez de um sistema. E essa possibilidade de rastreabilidade também não é consentânea com a ideia de minimização de uso de dados e redução de riscos presentes na LGPD. Ela inclusive vai contra um pressuposto fundamental da aplicabilidade da *privacy by design*, da privacidade na concepção, que é a utilização de recursos, como criptografia, no sentido máximo, que hoje em dia parece senão tecnologias uniformemente adotadas algo o mais próximo disso.

Mesmo a utilização restrita de técnica de rastreabilidade para grupos, que, eventualmente, possa ser pleiteada, é hipótese que, eventualmente bem-intencionada, não é necessariamente eficaz, pertinente nem sequer atinente à ideia da LGPD de que, hoje em dia, a privacidade não é um direito individualístico, não é um direito egoístico, por excelência, um direito

que concerne somente a um indivíduo. Grupos, principalmente grupos em situação de vulnerabilidade, em situação de minoria, ainda mais em situações politicamente delicadas, como a que vemos hoje em vários pontos no globo, podem se ver especialmente prejudicados por medidas como essa.

A própria LGPD, quando acena ao princípio da não discriminação como um dos seus princípios fundamentais, faz aceno à privacidade coletiva, à privacidade de grupos. Lembro sempre que a privacidade, hoje em dia, é um direito instrumental, é um passo necessário, imprescindível para tantos outros direitos, como a liberdade de associação, alguns mais concretamente colocados aqui, mas a própria liberdade de expressão, de informação, enfim, e o desenvolvimento da personalidade e de ideias coletivamente arregimentadas é necessário.

Outro ponto que eu gostaria de tratar — lembro que temos pouco tempo aqui — é o da impropriedade de aplicação de soluções diretamente trazidas de experiências estrangeiras que eventualmente nem sequer foram testadas, nem implementadas completamente no estrangeiro. Aqui eu faço menção à lei alemã referente à moderação de conteúdo em redes sociais, a NetzDG, que vem sendo colocada como exemplo, quase num arroubo de uma figura retórica, quase uma sinédoque — isto é, toma-se uma parte do que se trata aqui no PL como um todo. A NetzDG, como a própria Profa. Clara Keller já deixou muito claro, não trata de toda a Internet, trata somente de redes sociais. Ela não se aplicaria, portanto, a mecanismos de mensagísticas. Além disso, ela tem crivos muito fortes, muito concretos, no sentido de estabelecer como passivo de moderação somente conteúdos que sejam definidos como crime perante o código penal alemão, limite que não existe na nossa legislação.

E aqui já me encaminho para as conclusões. Como o nosso tema é proporcionar alternativas e não somente apontar problemas, lembro o que foi dito por Alex Stamos, que já foi responsável pela segurança do Facebook. Ele disse, certa vez, com muita propriedade, que o objetivo das mensagens direcionadas — no fundo, o que se procura é o tratamento de dados para a entrega de conteúdo e outros pontos — não é propriamente, muitas vezes, enviar uma mensagem em si, mas arregimentar uma audiência, organizar uma audiência. Muitas vezes, mais e além do combate estrito às *fake news*, está também a proteção de dados, com uma função importante, no sentido de que as audiências não sejam desmesurada e ilegitimamente colocadas.

Há alternativas, sim, que podem ser apresentadas, para legitimar e funcionar em conjunto com os sistemas de moderação de conteúdo. Eles se baseiam em sistemas operativos, com fácil *design* e implementação, referentes a denúncias de usuários, que podem ser utilizadas para aferição de potenciais agentes maliciosos, análises de metadados, o que, muitas vezes, vem sendo deixado de lado em algumas análises. Enfim, há muitas alternativas que não quebram necessariamente o equilíbrio e esse pacto social que é a LGPD. Elas devem ser levadas em consideração.

Sempre lembramos que algumas alternativas colocadas à mesa apresentam riscos e arestas muito mais contundentes e potencialmente danosas a esse novo pacto social e à modernização que promove a LGPD e a proteção de dados no nosso sistema jurídico.

Muito obrigado, Deputada.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Danilo, nós é que agradecemos. Tenho certeza de que o senhor tem muito mais para contribuir, em virtude do pouco tempo que lhe foi concedido. Sua participação é sempre importante na construção dessa legislação, como foi com a Lei Geral de Proteção de Dados. Fico muito feliz em recebê-lo aqui. Gostaria de fazer esse registro.

Passo a palavra, pelo tempo de 10 minutos, à Sra. Jaqueline Abreu, pesquisadora e membro da Comissão de Juristas PDP — Proteção de Dados Pessoais. *(Pausa.)*

Deve ter havido alguma interferência.

(Não identificado) - Eu acho que caiu a comunicação, Presidente. Pode passar para outro convidado. Depois ela retorna.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Então, passo a palavra à Sra. Miriam Wimmer, Diretora da Autoridade Nacional de Proteção de Dados.

É um prazer recebê-la aqui.

A SRA. MIRIAM WIMMER - Muito obrigada. É um prazer enorme para mim estar aqui.

Presidente, agradeço a V.Exa. o convite para participar deste painel junto com expositores tão ilustres e a todos os Deputados e Deputadas autores dos requerimentos para a realização desta audiência pública.

Queria começar fazendo logo um *disclaimer*, Deputada. Eu sou atualmente Diretora da Autoridade Nacional de Proteção de Dado, mas esse tema é bastante recente também para nós. De modo que não existe ainda uma deliberação do Conselho

Diretor da ANPD quanto ao tema. Trago aqui uma avaliação preliminar, a partir de uma ótica pessoal. Naturalmente, os demais diretores podem eventualmente ter visões um pouco diferentes.

É importante lembrar que, quando tratamos da desinformação, esse fenômeno é realmente multidimensional, com uma série de causas: econômicas, sociais e políticas. Desse modo, o enfrentamento desse fenômeno requer também uma abordagem multidimensional. E a proteção de dados pessoais é justamente um desses olhares que deve ser somado a outros. Naturalmente, quando estamos lidando com esse fenômeno, é preciso levar em consideração também os diversos valores constitucionais que se buscam proteger, como, por exemplo, a liberdade de expressão, os direitos de participação política, a qualificação do debate público, além da própria privacidade e proteção de dados pessoais, que ganha, inclusive, *status* de direito fundamental autônomo.

O evento de hoje está voltado para discutir o tema da identificação de agentes maliciosos. Parece-me importante, logo de partida, destacar que, justamente pela multidimensionalidade desse fenômeno, há uma pluralidade de estratégias regulatórias que têm sido perseguidas em outros países, como: estratégias voltadas, por exemplo, para a educação; *fact-checking; media literacy* para tecnologia, em termos da redução da velocidade de disseminação de notícias enganosas; aspectos relativos a incentivos financeiros; questões ligadas à transparência; sinalização de contas inautênticas; critérios para remoção de conteúdo.

Quando tratamos de repressão, aspecto que nos reúne aqui hoje, parece-me importante ter em mente que, justamente, por estarmos lidando com o fenômeno que está estreitamente conectado à liberdade de expressão, é que nossa abordagem deve ser necessariamente cautelosa. Não custa lembrar que o próprio STF, no âmbito da ADPF 130, que julgou a inconstitucionalidade da Lei de Imprensa, estabeleceu haver uma posição preferencial da liberdade de expressão em face de outros direitos fundamentais. Esse é um olhar que deve também pautar o presente debate.

Tendo feito tal consideração, eu queria falar um pouquinho sobre a contribuição que a legislação de proteção de dados pessoais traz para o tema. E é importante salientar que a LGPD não é uma norma *antifake news*. Muito embora ela tenha uma contribuição a dar, não é uma norma que busca traçar parâmetros para remoção de conteúdo ou para avaliação da fidedignidade ou veracidade de conteúdos que circulam na Internet. Pelo contrário, essa é uma norma que traz uma contribuição muito mais sistêmica para endereçar esse fenômeno, porque ela trata da forma como os dados pessoais fluem no ambiente analógico e no ambiente digital.

De fato, é preciso lembrar que, atualmente, talvez o principal problema da desinformação não seja propriamente conteúdo enganoso, que é algo que sempre existiu, mas, sim, a forma de circulação desse conteúdo, a possibilidade de elaboração e disseminação de conteúdo de maneira direcionada àquelas pessoas que são mais suscetíveis a serem influenciadas por tais de argumentos. E isso se liga a um fenômeno mais amplo de personalização, de granularidade da comunicação, ao uso mais intenso de técnicas de *marketing* comportamental, que são necessariamente acompanhadas da formação de perfis de titulares de dados. É o tratamento algorítimico de dados pessoais.

Nesse sentido, a contribuição que a LGPD traz não diz respeito ao conteúdo que circula nas redes, mas, sim, à forma como tais mensagens são endereçadas a destinatários específicos.

O Prof. Danilo já mencionou aqui o papel da proteção de dados pessoais como viabilizador de outros direitos: liberdade de expressão, de associação, de defesa de posições políticas, de participação em processo de liberação pública. Nesse sentido, é importante lembrar também dos princípios trazidos pela LGPD, em particular, os princípios da finalidade, da adequação e da necessidade. Isso porque esses princípios indicam que o tratamento de dados deve se dar para finalidades específicas. Há limitações quanto ao uso secundário de dados pessoais para finalidades distintas daquelas que justificaram a sua coleta. O tratamento deve ser adequado à finalidade inicial e, sobretudo, não deve ir além daquilo que é estritamente necessário para atingir tal finalidade. Não se devem coletar mais dados do que o necessário, simplesmente porque o tratamento de dados suscita novos tipos de riscos para os titulares.

É importante ressaltar que até mesmo os dados que são publicamente disponíveis, tornados públicos pelos próprios titulares, são protegidos pela LGPD, inclusive quanto aos direitos dos titulares e as finalidades de uso de tais dados. Nesse sentido, a LGPD é uma norma muito poderosa para incidir sobre esse tema, na medida em que ela pode limitar, por exemplo, determinadas práticas de formação, de venda ou de compartilhamento de dados pessoais muitas vezes utilizados na disseminação de notícias falsas ou enganosas.

E eu queria focar o tema do painel de hoje, falando da identificação de agentes maliciosos, e mencionar, a partir de uma perspectiva pessoal, que há várias propostas na mesa quanto à rastreabilidade de mensagens e à necessidade de identificação de indivíduos no uso de redes sociais.

Eu sugiro novamente que a leitura da LGPD nos impõe a necessidade de que a abordagem seja cautelosa. Especialmente, o princípio da necessidade, sobre a minimização da quantidade de dados pessoais que são tratados e coletados, indica

que precisamos ter um olhar cuidadoso quanto à instituição de novas regras de identificação, de novos mecanismos de rastreamento de mensagens, por exemplo, justamente porque o aumento da coleta de dados pessoais pode ensejar maiores riscos, maiores vulnerabilidades no fim das contas, principalmente no que tange à privacidade, à proteção dos dados pessoais dos titulares.

Por fim, nos poucos minutos que me restam, nesta fala super-rápida, eu quero tratar das competências da ANPD e da própria LGPD.

A discussão em curso no Congresso Nacional deve necessariamente ser construída com base naquilo que já foi pactuado no âmbito da própria discussão da LGPD, reconhecendo o papel que a ANPD tem a desempenhar nesse contexto. Vale lembrar aqui algumas competências da ANPD: propor medidas de prevenção e de segurança; avaliar a transparência do tratamento de dados efetuados pelas plataformas digitais, incluindo o compartilhamento de dados e uso para propaganda direcionada; garantir os direitos dos titulares. A lei impõe também à ANPD um papel ativo, em termos de cooperação e coordenação com outros órgãos dotados de competência correlatas. Destaca-se aqui, por exemplo, o papel do Tribunal Superior Eleitoral, com quem já estamos em conversas iniciais.

Salientaria sobretudo o papel da ANPD em termos de orientação, promoção do conhecimento, estímulo a padrões que facilitem o controle pelos titulares. O Prof. Danilo, por exemplo, já falou do *privacy by design*. É mais um papel que pode ser desempenhado pela ANPD no enfrentamento desse fenômeno.

Já concluindo, dentro do tempo estabelecido, parece-me que a discussão sobre o projeto de lei que trata da desinformação deve necessariamente buscar uma abordagem que seja proporcional, avaliando que eventuais restrições ou exigências adicionais de identificação, de rastreamento de mensagens, devem ser aquelas necessárias, proporcionais, para atingir finalidades específicas. Deve-se buscar preservar esse núcleo fundamental de direitos fundamentais, tanto de proteção de dados pessoais como de liberdade de expressão.

Eu acrescento que quando se pensa em novas regras é preciso avaliar não apenas o seu efeito pontual, mas sobretudo o seu efeito sistêmico no ambiente digital, avaliando suas consequências de maneira mais ampla com a coletividade que faz uso desses meios para se comunicar, expressar suas posições e participar do debate público.

Exma. Sra. Presidente, concluo minha fala inicial e fico à disposição para responder eventuais perguntas posteriormente. Agradeço mais uma vez a oportunidade.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Miriam, muito obrigada pela sua participação. É muito importante o que a senhora disse.

Sei que o tempo disponibilizado é pouco. Vou avaliar o tempo de 10 minutos, porque os senhores têm muito a contribuir com o trabalho do nosso Relator e com o meu também.

Eu acho que a Sra. Jaqueline ainda não voltou.

(Não identificado) - Presidente, ela já retornou.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Peço desculpas.

Eu gostaria de passar a palavra, pelo tempo de 10 minutos, à Sra. Jaqueline Abreu, pesquisadora e membro da Comissão de Juristas PDP — Proteção de Dados Pessoais.

A SRA. JAQUELINE ABREU - Bom dia a todos.

Gostaria de agradecer ao grupo de trabalho o convite e, na pessoa da Deputada Bruna Furlan, dizer que é uma honra fazer parte deste diálogo, ainda mais com colegas que eu tanto admiro.

Também peço desculpas pelo meu pequeno problema de conexão.

Eu falo aqui hoje da minha capacidade como pesquisadora. Desde 2003 eu venho estudando privacidade, proteção de dados e os conflitos que se colocam pelo interesse em garantir eficiência em investigações criminais, promover segurança pública. No ano passado, eu tive a oportunidade de participar da Comissão de Juristas formada pela Câmara dos Deputados, inclusive com o Prof. Danilo, para debater e elaborar um anteprojeto de lei para proteção de dados aplicada a investigações criminais em segurança pública. Nós já lidávamos com o tema da sessão de hoje, que é como combater agentes maliciosos sem ir contra o princípio de proteção de dados.

Nesse contexto, eu tenho três breves pontos para tratar.

O primeiro deles é que a legislação brasileira já prevê hoje diversos mecanismos de investigação que se aplicam, naturalmente, para apurar delitos que ocorrem na Internet ou que se aproveitam da Internet. Nós temos desde as requisições judiciais de registro segundo o marco civil, que a Internet garante desde 2014 e servem para identificar usuários não imediatamente autenticados com os nomes reais. Há também a possibilidade de fazer quebra de sigilo de contas,

interceptações telemáticas, tudo isso apoiado por outros mecanismos tradicionais, como a quebra do sigilo bancário, quando necessário para seguir o dinheiro — *following the money* —, ou buscas e apreensões em locais que estejam relacionados ao crime.

A Internet está longe de ser terra de ninguém, e já há vários mecanismos de combate ao crime à disposição. De certo modo, o que existe hoje, que, por vezes, prejudica o trabalho policial, em grande parte, são problemas que já existiam antes da Internet: falta de capacidade técnica ou de recursos e até de preparo do pessoal para fazer um trabalho investigativo de qualidade, considerando a complexidade do que está posto. Isso acaba alimentando falsamente a percepção de que nós estamos muito atrás, de que nós precisamos de novos meios tecnológicos para combater o crime, quando, na verdade, há muito a aperfeiçoar em termos de eficiência com o que já existe, sem precisar alterar a legislação para criar novos meios de obtenção de provas.

O segundo ponto diz respeito diretamente às propostas que o PL 2.630 traz para identificação de agentes maliciosos *on-line*, notadamente esse que já vinha sendo tratado, o art. 10, e a ideia de rastreabilidade. Esse dispositivo vai na contramão de princípios de proteção de dados, porque obriga uma retenção massiva de dados pessoais vinculada ao conteúdo do que é dito. Não dá para verificar se o conteúdo será enviado para mais de cinco pessoas, ou até mil vezes, ou mais do que mil vezes, sem etiquetar tudo o que está sendo dito.

Isso esbarra no princípio, como já vinham dizendo meus colegas, da necessidade da minimização, ao mesmo tempo em que intervém em aplicativos que desenharam os próprios sistemas para observar a privacidade, para que esses aplicativos, então, passem a coletar mais dados do que o necessário e se transformem em ferramentas hábeis de vigilância sobre as comunicações, ou seja, vai contra também a privacidade por concepção, como já diz o Prof. Danilo.

Eu entendo que desinformação é um problema. Isso é claro. Eu entendo também que, hoje, os mecanismos de mensageria privada começaram a ser subutilizados como meio de comunicação de um para muitos, com forma de comunicação pública. E eu consegui entender a teoria de que seria interessante se a polícia pudesse, diante de uma mensagem, de um vídeo ou de um áudio que seja criminoso, identificar de onde aquilo veio, quem foi que colocou aquilo na rede, e assim, supostamente, desbancar uma organização criminosa porventura envolvida. Mas há problemas nessas premissas do início ao fim, que tornam essa uma proposta ruim, não só do ponto de vista da proteção de dados, mas do ponto de vista de política pública, de política criminal. Primeiro, porque a observância de princípios de proteção de dados pessoais e o respeito à criptografia de ponta a ponta, sua integridade, é um mecanismo de prevenção de crimes. Quando nós colocamos isso a perder, estamos fragilizando, vitimizando pessoas em outras pontas.

A segunda ideia é que temos dificuldade hoje para combater desinformação feita à plena luz do dia por pessoas que não só já estão identificadas, como são plenamente conhecidas em seus perfis públicos. Também temos dificuldade de concordar sobre o que é uma informação falsa. Por vezes, nós vemos mecanismos jurídicos, como difamação e calúnia, serem movidos contra pessoas abusivamente. Então, parece-me um pouco fantasioso achar que criar esse mecanismo de vigilância massiva só vá servir para ser usado legitimamente e pegar quem produziu *fake news*, e que não seria usado para criminalizar pessoas que estão usando uma ferramenta digital legitimamente com movimentos sociais.

A terceira ideia é que atores sofisticados, supostamente aqueles que criam a necessidade de um mecanismo assim, continuarão tendo meios para divulgar conteúdo ilícito nesses mensageiros. Eles poderão, por exemplo, simplesmente utilizar-se de estratégias de envio de mensagens de fora do Brasil ou usar os limiares indicados, como as instruções sobre o que fazer, deixar de mandar mensagem mais de 5 vezes em 15 dias, mandá-las de forma "copia e cola" ou fazer pequenas alterações do conteúdo.

Esse me parece um problema fatal de adequação dessa medida ao seu propósito. Se não estamos sendo capazes de pegar efetivamente quem importa para desbancar essas redes de desinformação, ou se pegarmos no máximo um grupo não relevante de pessoas, como meu tio e minha tia, o nosso avô e a nossa avó, que pegaram conteúdo de uma rede e jogaram na outra, eu não entendo ser possível justificar a criação dessa infraestrutura de monitoramento preventivo que interfere em direitos fundamentais. Nós estaremos implicando pessoas criminalmente à toa, por coisas pequenas, não vamos pegar os peixes grandes e ainda vamos gerar um enorme efeito inibidor sobre a liberdade de expressão, porque as pessoas podem recear cair nessa cadeia de encaminhamentos para compartilhar informações.

A última ideia é que, na Comissão de Juristas, nós chegamos ao diagnóstico do problema em relação ao art. 10 e, de lá, chegou a sair uma redação alternativa, que permitiria a preservação prospectiva de registros de interações de contas — quem mandou mensagem para quem, quando contas específicas são suspeitas de estarem sendo movidas ou gerenciadas para práticas de crimes. Do ponto de vista da proteção de dados pessoais, isso é mais atraente, porque é um mecanismo direcionado e não massivo de retenção, e não interfere na criptografia de ponta a ponta. Por isso, seria compatível.

Ao mesmo tempo, eu faço a advertência de que esse tipo de dispositivo teria um impacto muito maior em investigações em geral, de tráfico de drogas, corrupção, abuso infantil, para além de problemas de desinformação. E, sob essa perspectiva geral, então, precisaria ser analisado.

Parece-me que até antes de uma alternativa que gerasse tanta preocupação como a do atual art. 10 do PL, eu não acredito que havia uma demanda forte de agentes policiais por algo assim. E penso que se criou essa versão alternativa mais compatível com os direitos fundamentais, porque a alternativa que está posta é realmente muito ruim. Mas nem por isso, automaticamente, algo precisa ser acolhido sem ampla discussão. Eu, na verdade, diria que nós não deveríamos criar mais meios de obtenção de provas invasivos sem uma lei geral de dados que se aplique a investigações criminais e segurança pública. Nós precisamos avançar nessa frente, antes ou paralelamente, para pensar nesses novos dispositivos. Essa deveria ser uma prioridade também. De todo modo, para finalizar, parece-me que, em relação a questões que movem as preocupações com desinformação em mensageria privada, é preferível apostar em mecanismos de transparência, inclusive com incentivo à adoção de medidas para impedir que esses aplicativos ganhem as características de meio de comunicação de massa, incentivo à limitação de transmissão, combate ao comportamento inautêntico, combate ao uso de *software* de disparo em massa, construção de diálogo institucional com provedores e construção de canais de resposta mais rápidos. Parece-me que a solução está por aí.

Com isso, eu chego ao fim desta minha fala inicial e fico à disposição para responder a perguntas, inclusive sobre outros aspectos que possam surgir.

Muito obrigada.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Jaqueline, muito obrigada por sua participação. É muito bom ouvi-la.

Passo a palavra à Sra. Bruna Martins dos Santos, representante do Data Privacy Brasil. Devo dizer que estou feliz em reencontrá-la.

A SRA. BRUNA MARTINS DOS SANTOS - Obrigada, Deputada.

Bom dia a todos e a todos.

Eu gostaria de começar cumprimentando os Parlamentares do GT de aperfeiçoamento da legislação brasileira, na pessoa da Deputada Bruna Furlan, e dizer que é uma honra, de fato, participar desta Mesa com tantos colegas que tenho como referências pessoais.

Eu sou Bruna e atuo como Coordenadora de Incidência na Associação Data Privacy Brasil de Pesquisa.

Para lhes apresentar a instituição, esclareço que o Data Privacy Brasil é um espaço de articulação entre duas instituições: o Data Privacy Brasil de Ensino, instituição privada que se dedica à difusão do conhecimento sobre privacidade e proteção de dados pessoais, e a Associação Data Privacy Brasil de Pesquisa, organização não governamental voltada para a produção de pesquisas e incidência no debate público sobre privacidade e proteção de dados pessoais, onde também trabalho. A associação de pesquisa é membro da Coalizão Direitos na Rede, coletivo que reúne mais de 47 entidades que trabalham no campo dos direitos digitais no País. Tenho certeza de que os senhores já ouviram algumas delas no contexto dessas audiências.

Partindo para os pontos da minha intervenção na audiência de hoje, começo com um pouco de conjuntura. Para nós do Data Privacy Brasil parece fundamental que o combate à desinformação caminhe de mãos dadas com o debate sobre proteção de dados pessoais, a fim de que obtenhamos soluções que não minimizem os danos ao direito autônomo à proteção de dados pessoais que eventuais iniciativas legislativas possam oferecer.

No entanto, essa é uma discussão que começou um pouco antes da entrada em vigor da nossa Lei Geral de Proteção de Dados Pessoais e também da criação da própria ANPD, que a Miriam aqui representa. E sobre isso vale dizer, como manifestaram o Danilo e a Miriam, que, além de termos uma lei que reforce os princípios norteadores das atividades de tratamento, como finalidade e proporcionalidade, e que também limite o uso secundário de dados, é fundamental que reconheçamos o caráter central da ANPD nesse debate, nesse ecossistema, para reforçar dispositivos necessários para a garantia de direitos, a agenda dos direitos titulares, de maneira geral, de forma conjunta com entidades como o próprio Supremo.

Então, enquanto o País começa a dar os primeiros passos para a criação de uma cultura de proteção de dados, é importante também que a nossa autoridade e mais espaços sejam envolvidos nessa discussão.

Partindo mais diretamente para o tema, começo retomando um posicionamento recente da Relatora Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão da ONU, Irene Khan, ao dizer esses dias que a desinformação é, sim, um fenômeno que mina a liberdade de expressão e as instituições democráticas, ajuda na polarização

de debates políticos e alimenta a desconfiança pública. No entanto, algumas das medidas implementadas pelos Estados até hoje são desproporcionais e existe uma incidência muito alta de leis amplas, com definições vagas e que acabam criminalizando, restringindo ou censurando a fala *on-line*. Essas medidas também têm um resultado quase imediato, que é o de desencorajar fluxos de informação. Ao mesmo tempo, quando desencorajamos esses fluxos, acabamos alimentando mais rumores do que aqueles que queríamos combater inicialmente.

Em um segundo momento, Irene fala de pontos que já foram abordados nesta audiência também. Ela conta que algoritmos, publicidade direcionada e práticas de coleta de dados das maiores empresas de rede social também estão levando os usuários a compartilhar ou ter acesso a conteúdos extremistas e teorias da conspiração, mas também, no limite, eles enfraquecem os indivíduos, de maneira geral, e roubam a autonomia para desenvolver livremente suas opiniões. Nessa fala recente, a Relatora também aponta que algumas das medidas relativamente positivas para banir ou reduzir impacto da desinformação não foram suficientes até o momento e acabaram gerando problemas que eu já mencionei.

Só para falar também do *microtargeting*, casos como o do Cambridge Analytica, de alguns anos atrás, demonstram que a ausência de marcos legais para a proteção de dados pessoais, somada a essas práticas de coleta massiva de dados para fins de impulsionamento de conteúdo eleitoral ou desinformativo, são eventos que facilitam bastante a manipulação da sociedade. Então, nesse ponto, é chave que já tenhamos aprovado uma Lei Geral de Proteção de Dados.

Falando mais diretamente do PL 2.630, vou comentar pontos relativos a alguns artigos. Começo sobre a discussão de aumento de obrigações acerca de coleta de dados pessoais de usuários de plataforma. Artigos como o 7º colocam que a identificação de contas pode ser feita em casos específicos, como denúncias por desrespeito à lei, contas automatizadas não identificadas como tal, contas inautênticas e em caso de ordem judicial. Um ponto que eu queria colocar sobre essa questão é que o incentivo para que essas plataformas desenvolvam medidas para detectar fraudes no cadastro dessas contas pode também ser interpretado como uma espécie de poder de polícia desproporcional conferido a elas.

Isso pode também incentivar que, para cumprir a lei, essas plataformas acabem aumentando as atividades de coleta de dados pessoais de maneira genérica para poder ter esses dados em caso de uma ordem judicial ou de uma solicitação. Então, como está redigido atualmente o art. 7º pode deixar os usuários dessas plataformas mais vulneráveis a vazamento de dados e abusos no uso do documento de identidade ou na prática de perfilamento, que já comentei que são usados normalmente para disseminação de desinformação.

Partindo para a questão da rastreabilidade, e muitos aqui já se manifestaram sobre isso, é importante reforçar que os métodos de rastreamento de mensagens compartilhadas para finalidade de identificação do usuário ainda se demonstram ineficazes. Entre alguns pontos falhos sobre essa discussão, há a ideia de que é possível identificar o ator de conteúdo ilícito circulando exclusivamente em uma plataforma. Nós já vínhamos comentando há alguns anos — e, há quase 1 ano, com a Coalizão Direitos na Rede — que a desinformação tem uma característica multiplataforma. Então, são conteúdos que se iniciam no Youtube e vão acabar no WhatsApp. Essa característica é uma limitadora de que possamos, de fato, encontrar os autores dos conteúdos, além de ser uma medida que coloca a criptografia em risco.

Adicionalmente, as medidas de criação de sistemas rígidos para padronização de rastreabilidade de mensagens podem gerar oportunidades e tentativas de *game the system*. Então, são atores que tentam burlar esse sistema por vários meios também. Em nossa opinião, essa análise de custo-benefício mostra-se relativamente frustrada. As vantagens não são grandes o suficiente para que coloquemos, de fato, a segurança dos usuários dessas plataformas em risco, e a rastreabilidade é uma medida que afeta, sim, um número grande de jornalistas, ativistas, pessoas comuns. Ela vai vulnerabilizar essas pessoas.

Em relação à sensibilidade na discussão de metadados, eu queria só colocar que, mais para o final, passaremos a falar também do Marco Civil. Vale lembrar que metadados são mecanismos que constroem um cenário de comunicação, sem se revelarem necessariamente no conteúdo da mensagem. Entretanto, eles também são parte de um processo, de envelopar conteúdos. No limite, a coleta de metadados também pode permitir que identifiquemos pessoas por parte de informações agregadas. Então, a retenção preventiva indiscriminada de metadados flexibiliza também garantias constitucionais, considerando toda uma população como suspeita, e entra em uma rota de colisão, com princípio de presunção de inocência dos indivíduos.

Nesse ponto, eu também queria colocar a tentativa de obtenção e retenção de metadados, em especial, a tentativa de obtenção de dados de porta lógica, que não é tecnologicamente neutra e colide com algumas das garantias asseguradas no Marco Civil da Internet. Falando do Marco Civil — acho que a Jaqueline já tratou muito bem disso —, essa é uma lei que traz mecanismos suficientes o bastante para a identificação de usuários, para a persecução penal e para que, de fato, as atividades de investigação sejam realizadas. Esses mecanismos somados com outros, como interceptação telefônica e quebra de sigilo bancário, são suficientes quando há vontade política de se investigar conduta maliciosa.

Para encerrar, eu queria colocar, mais uma vez, que este debate sobre identificação de agentes maliciosos e medidas de combate à disseminação de desinformação, de fato, tem que caminhar de mãos dadas com a proteção de dados pessoais. Ambos são fundamentais para a proteção de indivíduos e proteção da nossa democracia. Aqui há discussões muito interessantes, como a do Canadá, em que se propõe um alinhamento entre a autoridade nacional de proteção de dados e as demais instâncias de verificação e acompanhamento de disseminação de desinformação, para o desenvolvimento de soluções e remédios para o combate desse efeito, com uma constante atenção ao tema de proteção de dados pessoais. Acho que o caso da DPA do Canadá é bastante relevante nesse cenário.

Aqui também o esforço de atuação legislativa deve mirar em como os dados pessoais dos cidadãos potencializam o direcionamento de propagandas políticas e campanhas de desinformação. Então, também precisamos proteger esses usuários de maneira geral.

Por fim, sabemos que o controle da desinformação é um assunto urgente. Entretanto, em primeiro lugar, é importante que o PL abandone dispositivos, como o artigo de rastreabilidade, que possibilitou a interpretação de uma relativa inversão do princípio de inocência. Também a necessidade de condução de investigações ou identificação de agentes maliciosos não deve colocar jamais em risco a criptografia ou limitar o uso de ferramentas que garantem a nossa privacidade *on-line*.

Peço, então, a atenção do grupo de trabalho, da Relatora e da Deputada Bruna Furlan com relação a esse tema, para que avancemos nele sem violar a privacidade e o direito autônomo à proteção de dados.

Muito obrigada.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Bruna, muito obrigada pela sua participação. Como sempre, são muito pertinentes os seus comentários.

Antes de passar a palavra à Sra. Samara Castro, gostaria de agradecer a presença aos nossos Parlamentares — todos sempre muito atuantes e participativos —, Deputada Lídice da Mata, e Deputados Rui Falcão e Gustavo Fruet, que estão em plenário. Eu quero dizer a V.Exas. que terão a palavra sempre que desejarem, ou antes ou após a fala dos nossos expositores.

Eu gostaria de passar a palavra à Sra. Samara Castro, membro do Instituto Nacional de Proteção de Dados, que também participa de comissão da OAB do Rio de Janeiro.

Tem a palavra a Sra. Samara Castro.

A SRA. SAMARA CASTRO - Bom dia. Obrigada, Deputada.

Primeiro, eu gostaria de agradecer a oportunidade de contribuir com este debate, que é tão relevante, e agradecer também a todos os Deputados e Deputadas que estão possibilitando este espaço de consulta e de escuta atenta nesta audiência pública, em todas as outras audiências que a antecederam e nas que vão acontecer ainda.

Este debate sobre como identificar os agentes maliciosos sem ferir a proteção de dados talvez seja um dos mais desafiadores que nós travamos até agora, e que ainda vamos travar. Também o considero como um dos mais atuais.

A proteção de dados é fundamental na luta contra a desinformação. E a exigência de maior transparência e responsabilidade no ecossistema de dados é uma chave para reorientar o modelo de negócios da economia digital baseado em anúncios. E é esse tipo de clareza que permite à população, muitas vezes vítima, e não agente da desinformação, construir um juízo de valor próprio sobre as informações que lhes são dirigidas. E isso é mais simples quando pensamos nas redes abertas, como as redes sociais, e muito mais complexo quando pensamos em termos de mensageria privada.

Eu gostaria até de reforçar uma abordagem que, muitas vezes, é tabu entre os pares, mas para mim é fundamental, para que tenhamos sucesso na identificação sem ferir a proteção de dados. Quando pensamos em aplicativos de mensageria privada, é importante definirmos critérios para uma separação séria entre o que é comunicação interpessoal, que merece e precisa de certas proteções, e o que é comunicação de massa, comunicação viralizada. Talvez um critério interessante — essas duas comunicações existem hoje dentro dos aplicativos de mensageria privada — fosse o da porta de entrada, uma vez que os grupos de WhatsApp, de Telegram, de *links* públicos não deveriam ter a mesma proteção que os grupos privados, os grupos de família, os de amigos, os profissionais, enfim.

Como o nosso desafio é buscar caminhos de identificação dos agentes maliciosos sem ferir a proteção de dados, o melhor espaço para que isso seja feito é dentro de um processo judicial, em que todos os direitos e garantias estejam assegurados.

No entanto, acabamos falando pouco sobre os aspectos processuais que envolvem essas batalhas judiciais. E aproveitando um pouco da minha experiência com esses desafios, porque sou advogada e atuo muito nesse tipo de demanda, eu quero trazer algumas contribuições nesse sentido. E vamos começar com o básico: uma conduta inadequada.

Quais são os mecanismos processuais que temos hoje para retirar um *post* do ar, para identificar um usuário responsável por uma publicação inadequada? E aqui estamos falando, realmente, de algo básico, nem são as grandes ofensas. Para

retirarmos um *post* do ar, identificar o usuário responsável por uma publicação, é necessária uma decisão judicial. E, geralmente, as pessoas acham que com apenas um *print* da publicação já é possível ter essa ordem judicial. Mas não é, o procedimento não é rápido, não é simples. A vítima ou a pessoa que deseja identificar o responsável pela desinformação, o comportamento ilícito ou criminoso, precisa ter a URL, o *link* que a publicação gera. Ela precisa decidir se vai apresentar esse processo na Justiça Comum ou no Juizado Especial. E se ela vai entrar na Justiça Comum, ela vai ter que arcar com as custas judiciais, caso não seja possível obter a Justiça gratuita. Mas a vantagem é que ela vai poder recorrer de algumas decisões. Já no Juizado isso não vai ser possível.

No Juizado, além de ela não ter custos, o trâmite vai ser mais célere. O processo termina mais rápido. Mas ela não vai ter espaço para produção de prova necessária para identificar justamente quem publicou o conteúdo ilícito, para depois ela, eventualmente, entrar com uma futura ação criminal indenizatória. Então, muitas vezes, ela ganha, mas não leva. Ela tira aquele conteúdo do ar, mas não se identifica o autor, o que acaba sendo prejudicial para a discussão que estamos fazendo aqui, a identificação dos agentes maliciosos. Assim, esse comportamento acaba sendo reproduzido e se permite que ele continue nas redes, com a sensação de não punibilidade das pessoas que reproduzem essas informações nas redes sociais.

Essa produção de prova para identificação do usuário não é uma tarefa simples, porque é necessária a ordem judicial para que a empresa de aplicação da Internet forneça o endereço de IP do *link* indicado. Depois, o autor da ação precisa conferir em um *site* específico qual é a empresa de conexão, a telefônica daquele IP. E essa identificação do usuário do IP só ocorre após o pedido para que a empresa de conexão quebre o sigilo dos dados, desde que tudo isso tenha sido autorizado.

Percebo que os senhores já perderam o fôlego aqui, não é? Imaginem quando temos centenas de IPs para conferir, quando há, por exemplo, um ataque massivo, que muitos dos Deputados e Deputadas aqui presentes sofrem cotidianamente! É um procedimento burocrático, é um procedimento demorado. E se o prazo legal para a guarda dessas informações expira, não é mais possível identificar o usuário, muitas vezes, e muito menos o seu financiador, se foi o caso, o que por vezes é comum, uma vez que o Judiciário é abarrotado de ações. Então, é comum, muitas vezes, não conseguirmos, efetivamente, fazer a identificação ao final das ações.

Eu sei que muitos dos Srs. Deputados e das Sras. Deputadas entendem muito bem o que eu estou falando aqui porque já passaram por essa situação.

Eu gostaria de aproveitar este momento para sugerir, como proposta ao projeto, que toda citação, intimação do Poder Judiciário para as empresas de aplicação na Internet, de conexão, se dê, obrigatoriamente, por meio eletrônico, porque hoje ainda não é assim. E que logo no pedido de medida liminar seja possível, junto com a ordem de indisponibilização do conteúdo violador de direitos, uma produção de prova mais célere na identificação do usuário por trás da postagem. Assim, na hora em que requerermos a identificação do IP, é preciso que no PL tenhamos um dispositivo legal que preveja o cruzamento automático dos dados com os provedores de conexão à Internet para o envio direto dessas informações pessoais dos usuários da ação judicial. E aí eu sei que já vai haver um rebuliço, o medo de que isso ofereça algum tipo de ofensa à proteção de dados.

Mas a ideia é que se crie um canal de interlocução entre os provedores de aplicação e os provedores de conexão para que, uma vez acionados para retirar do ar um conteúdo, automaticamente enviem o IP, que vai ser consultado dentro de um banco de dados, e esse IP seja informado diretamente nos autos do processo sem que exista esse compartilhamento. Assim, a proteção de dados vai estar assegurada e, ao mesmo tempo, vamos ter assegurada a garantia da identificação, sem perda de prazo e sem perda do direito daquelas pessoas que foram ofendidas. Esse procedimento tem que ser possível nos Juizados Especiais, para conferir agilidade à tramitação processual, além de assegurar, inclusive, a gratuidade para aqueles que não podem arcar com as taxas e as custas judiciais.

É preciso que haja a criação de instrumentos para a célere indisponibilização de conteúdo danoso e a identificação pronta dos usuários ofensores, para que as vítimas tenham realmente os dados necessários para entrar com ações de reparação de danos morais e até eventuais ações criminais. A criação desses instrumentos seria um esforço conjunto do Estado e das empresas para proteger os direitos dos usuários. Essa seria uma medida de baixo custo e de alto impacto que poderia constar nesse projeto. Ela traria menos danos aos usuários da Internet em geral, permitindo a identificação dos agentes maliciosos sem ferir a proteção de dados.

Eu sei que isso vai um pouco na contramão dos debates gerais que estamos fazendo, mas acho que é muito importante que falemos dos aspectos processuais, porque, querendo ou não, para que a identificação se dê de maneira a garantir o máximo possível de ampla defesa, de direito ao contraditório, de proteção de todos os aspectos efetivos, inclusive da proteção de dados, da privacidade, é importante que todo esse procedimento seja feito nos processos e dentro do sistema que temos hoje consolidado, que é o sistema judiciário.

Essa medida é efetiva e pode constar do nosso PL hoje. Isso seria superimportante. Realmente, é uma medida de baixo custo e de alto impacto, que garante a identificação dos agentes maliciosos sem ferir a proteção de dados.

Muito obrigada.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Samara Castro, muito obrigada pela sua participação.

Samara é membro do Instituto Nacional de Proteção de Dados e Vice-Presidente da Comissão de Proteção de Dados e Privacidade da OAB do Rio de Janeiro.

Agora eu passo a palavra, pelo tempo de 10 minutos, para o Sr. João Brant, Diretor do Instituto Cultura e Democracia.

O SR. JOÃO BRANT - Bom dia, Deputada Bruna Furlan; bom dia, colegas; bom dia, Deputados Orlando Silva, Rui Falcão e Gustavo Fruet. Inicialmente, eu queria agradecer o convite para participar deste debate.

Sou pesquisador em liberdade de expressão, comunicação e democracia há 20 anos. Minha fala parte de outro ângulo, diferente, tentando chegar a resultados que de fato respondam à pergunta proposta pelo debate de como identificar agentes maliciosos sem ferir a proteção de dados, mas partindo de outra leitura.

O Instituto Cultura e Democracia é recém-fundado. Os senhores podem procurar, mas vão encontrar, por enquanto, informações sobre ele. É um instituto que reúne uma série de pesquisadores e militantes desse campo também e passa a olhar essa questão da desinformação como um dos temas do seu foco.

Vou compartilhar minha tela, mas, antes, eu queria falar que parto aqui de uma visão de liberdade de expressão consolidada na literatura internacional, inclusive em decisões da Corte Interamericana de Direitos Humanos, que olha a liberdade de expressão como um direito individual e um direito coletivo. Ou seja, passamos a entender a desinformação como uma violação frontal à liberdade de opinião e expressão.

Isso dialoga um pouco com o relatório citado pela Deputada Bruna em relação à Relatora da ONU para Liberdade de Expressão. Mas isso também precisa ser entendido como uma violação do acesso à informação confiável, plural e diversa. Há decisões na Corte Interamericana respaldando essa visão. Eu acho que ela é fundamental para o nosso debate aqui.

Eu vou compartilhar minha tela e começo dizendo que eu vou fazer um roteiro aqui simples a partir de três problemas.

(Segue-se exibição de imagens.)

"Temos um problema?" — é a primeira pergunta —, *"Cenário atual"* e *"Quais as possíveis soluções?"* Eu acho que *"Temos um problema?"* é um problema de enorme gravidade e acho que essa é uma das questões centrais na hora de discutir proporcionalidade. Não é possível discutir proporcionalidade sem discutir qual é o problema que estamos enfrentando.

Eu trago alguns dados do Digital News Report, que são pesquisas feitas em janeiro e fevereiro deste ano. A maior parte dos brasileiros se informa via mídia *on-line* e redes sociais, então, mais do que TV. O Brasil hoje é líder em preocupação com informação falsa e enganosa: 82% dos brasileiros têm essa preocupação ante 37% na Alemanha. Entre os brasileiros, a leitura é que o WhatsApp é a principal fonte de informações falsas ou enganosas, quase o dobro do Facebook — números similares em países populosos do sul global, como Índia, Indonésia, Nigéria, África do Sul.

É muito diferente, por exemplo, dos dados no Reino Unido e nos Estados Unidos, países que costumamos observar como referência, que têm o Facebook em redes abertas com um número muito maior. Então, nós estamos falando de um fenômeno próprio de países populosos do sul global, cujas respostas precisam ser tomadas e geradas a partir da nossa realidade e não apenas olhando como referência soluções europeias ou americanas.

Além disso, existe um problema efetivo que impacta a realidade brasileira, impacta direitos sociais, impacta a democracia. Eu trouxe exemplos aqui — eu poderia trazer inúmeros — sobre levantamentos em relação à pandemia da COVID, em que 7 das 10 imagens mais compartilhadas sobre a pandemia em 522 dos grupos eram falsas — levantamento do Monitor WhatsApp da UFMG com a Agência Pública.

Levantamentos sobre o impacto nas eleições 2018 mostraram a rápida viralização de conteúdos falsos e a predominância de conteúdos falsos em grupos monitorados. Vale dizer que o WhatsApp tomou medidas importantes nesse período para aumentar o que eles chamam de fricção. Mas ainda assim estudos mostram que o problema permanece. Estudos dos próprios pesquisadores da UFMG envolvendo o Brasil, Índia e Indonésia mostram que, embora elas possam ser efetivas, são medidas para atrasar um pouco o espalhamento da informação, elas são inefetivas em bloquear a propagação de campanhas de desinformação em grupos públicos.

Então, no cenário atual — eu acho que isso a Samara, que me antecedeu, falou rapidamente —, nós estamos lidando com aplicativos de natureza híbrida e precisamos reconhecer essa natureza híbrida. Nós precisamos tentar identificar como justamente lidar com essa natureza híbrida. Esta é uma novidade dos últimos anos. Não existe na história da comunicação

de massa este volume com este impacto. Nós estamos falando de aplicativos que, ao mesmo tempo, carregam mensagens interpessoais privadas e mensagens virais ou potencialmente virais e de massa.

O problema é que essas funcionalidades não são separadas nem da perspectiva do serviço, nem da perspectiva regulatória, mas o paradigma regulatório de serviço privado é aplicado para todo o serviço. Ou seja, nós estamos cometendo um erro de guardar, utilizar todo o tema de proteção de dados, privacidade e confidencialidade e o aplicando a uma parte do serviço que não deveria ter necessariamente essa proteção.

É claro que alguns dirão que o número de mensagens com alta viralização é baixo relativamente, e é relativamente baixo. Enfim, os números que existem são os números do próprio WhatsApp e eles mostram que esse número é absolutamente muito alto.

Nós estamos falando da faixa de dezenas de milhões de mensagens virais todos os dias. Portanto, o impacto delas é perceptível pelo cidadão brasileiro entrevistado nas pesquisas; é perceptível pelos pesquisadores que atuam e monitoram o grupo de WhatsApp; e precisa ser considerado no debate, sob pena de estarmos ignorando uma realidade gritante do problema da desinformação no Brasil.

O resultado desse caráter híbrido, mas com tratamento especificamente privado, é que nós temos um ambiente opaco e majoritariamente anônimo, que impede hoje a responsabilização moral e legal, no caso do WhatsApp, a responsabilização moral especialmente; no Telegram, pode-se olhar isso de forma diferente, mas impede a responsabilização legal.

Nós não estamos falando só de um problema criminal e de grandes, vamos dizer assim, quadrilhas de desinformação. Nós estamos falando de pessoas comuns que não têm como proteger o seu direito civil, processar e pedir indenização. Eu teria inúmeros exemplos de jornalistas, ativistas de direitos humanos, pessoas assassinadas, cuja proteção da sua própria honra, da dignidade foi violada por causa de desinformação. E nós temos nesse caso um incentivo sistêmico à desinformação.

A saída está na separação da funcionalidade de comunicação interpessoal e comunicação viral de massa. Não há como enfrentar esse problema sem buscar essa separação e sem uma definição dada pela própria empresa ou pelo próprio usuário. Essa fronteira precisa ser desenhada em lei, o que de fato gera problemas, como já foi apontado aqui por alguns que me antecederam, mas nós precisamos lidar aqui. Ou faremos uma opção de ferir, em alguma medida, a liberdade empresarial e exigir que o serviço seja redesenhado para desenhar essa fronteira ou ela tem que ser feita por quem busca uma solução efetiva de impacto para isso.

Então, nós temos os seguintes cenários possíveis: não fazer nada ou apostar em soluções já existentes. Eu aqui discordo de alguns colegas que me antecederam em relação à eficácia de soluções já existentes. Eu acho que elas não são eficazes e não têm mostrado eficazes. Uma parte das propostas que estão como alternativa ao PL simplesmente legalizam algo que já é realizado hoje no âmbito do serviço e, informalmente, na relação da colaboração do WhatsApp com as forças de investigação.

Outra solução é o aprimoramento do art. 10 ou a modificação do art. 10. Eu quero trazer duas propostas nessa direção, buscando avançar e superar questões que estão postas hoje, sem ilusão, vale dizer, de qualquer bala de prata. Ou seja, nós não entendemos que essa defesa que vai ser feita de soluções para buscar isso seja solução que resolva todo o problema da desinformação ou que este em si resolva. Eu acho que ele mitiga, ajuda a resolver e ajuda a quebrar, porque o principal é quebrar um incentivo sistêmico à desinformação que hoje existe.

Em relação ao art. 10 hoje — eu não vou passá-lo aqui em detalhes —, eu tenho uma avaliação um pouco diferente da dos colegas que me antecederam. Eu acho que ele não tem exatamente um problema grave de desproporcionalidade, mas ele traz, sim, alguns problemas de retenção, que se pode chamar de excessiva de dados a partir de algumas leituras. Eu colocaria um contraponto a isso dizendo que hoje a Lei das Organizações Criminosas manda guardar metadados de telefonia por 5 anos e não vejo uma grita de que isso esteja violando direitos de privacidade tão grande como tem sido apontado nesse caso. Também traz uma possível ineficácia e um possível uso de dados em desconformidade com a lei.

Há possíveis aprimoramentos do art. 10: explicitar a destruição das mensagens que não se tornarem virais depois de 15 dias; definir que a obrigação não se aplica a mensagens que não sejam encaminháveis ou limitar o acesso para alguns casos.

Queria aproveitar que eu tenho apenas 40 segundos para apresentar uma proposta que considero alternativa, uma pequena modificação que os provedores de aplicação terão que fazer no sentido de oferecer ao usuário a condição de separar as mensagens entre interpessoais ou privadas. Ela limpa, vamos dizer assim, quase todos os problemas que foram apontados aqui em relação ao atual art. 10. Nós precisaríamos guardar apenas os metadados das mensagens passíveis de encaminhamento.

Eu peço 30 segundos só para terminar a apresentação, se possível.

Essa definição de mensagens passíveis de encaminhamento seria dada por uma solução técnica oferecida pelo serviço de mensageria privado e seria definida pelo próprio usuário remetente. Aí você poderia, sim, guardar apenas os dados do primeiro usuário remetente e apenas o quantitativo de usuários alcançados, para que se possa mensurar o dano no caso de qualquer avaliação de ilícito civil ou penal, mantida toda a questão do acesso apenas com ordem judicial.

Isso empodera o usuário, isso faz com que essa definição não esteja com o legislador, mas com o próprio usuário e com a empresa fornecedora do serviço. Não se afetam as mensagens interpessoais e não se tira uma lista de possíveis usuários alcançados, tira-se apenas o quantitativo deles.

Deixo essa proposta para consideração do GT e da Comissão, buscando soluções de que, acredito, todos nós estamos atrás.

Muito obrigado.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Eu que lhe agradeço. Muito obrigada pela sua participação.

Houve um probleminha sobre a minha presença no Infoleg e eu estava resolvendo, por isso, a minha câmera saiu um minutinho.

Katia, o nosso Relator está aí?

A SRA. KATIA DA CONSOLAÇÃO DOS SANTOS - Está, sim, na sala do Zoom.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Então, eu vou conceder a palavra ao nosso Relator. Antes, quero agradecer aos nossos expositores na pessoa do João Brant. Muito obrigada, João, pela sua participação. Muito obrigada a todos pela participação.

Eu gostaria de passar a palavra para o nosso Relator, o Deputado Orlando Silva. *(Pausa.)*

A SRA. KATIA DA CONSOLAÇÃO DOS SANTOS - Parece que ele não está na sala. O vídeo dele está aqui, mas acho que ele deve ter dado uma saída.

Temos dois Deputados aqui em plenário e mais dois na sala do Zoom. *(Pausa.)*

Ah, o Relator chegou.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Tem a palavra o nosso Relator, Deputado Orlando Silva.

O SR. ORLANDO SILVA (PCdoB - SP) - Sra. Presidente...

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Sim, Deputado. Eu ouço V.Exa. muito bem.

O SR. ORLANDO SILVA (PCdoB - SP) - Presidente, eu estou em deslocamento para Campinas, e ficou um pouco difícil aqui. Mas acompanhei todas as falas, do Danilo Doneda, da Jaqueline Abreu, da nossa Diretora da ANPD, a Miriam, da Bruna, da Samara e, agora, do meu amigo João Brant.

Inicialmente, Presidente Bruna, registro que essa audiência pública de hoje tem uma dimensão afetiva, eu diria, porque é um encontro com vários amigos e amigas. Mais do que especialistas e pesquisadores — como no caso da Miriam, que é uma autoridade pública —, eles são amigos, e falamos juntos no debate acerca da Lei Geral de Proteção de Dados Pessoais. Então, eu queria lembrar a V.Exa., que é a nossa chefe na coordenação aqui do projeto, que tem uma dimensão também afetiva a realização dessa reunião no dia de hoje.

Queria cumprimentar todos os colegas Deputados. Vejo aqui a Deputada Angela Amin, o Deputado Rui Falcão, a Deputada Lídice da Mata e o Deputado Gustavo Fruet, que acompanham essa audiência.

Queria dizer que eu concordo com a Dra. Samara quando ela diz que o tema da identificação dos agentes maliciosos sem violar a privacidade talvez seja um dos temas mais sensíveis que temos para enfrentar no esforço do combate à desinformação.

A Dra. Miriam tem razão quando diz que essa é uma matéria multidimensional. De algum modo, ela comunga com a visão apresentada pelo João Brant de que não há uma bala de prata, não há uma solução mágica, não há um estalar de dedos para que, a partir daí, positivados numa lei, nós encontremos o caminho suficiente para combater um fenômeno que é global e ganha formas diferentes, um aplicativo diferente, com tecnologias diferentes.

Não é simples um processo como esse. Quando observamos a desinformação em política, vemos que há, sim, influência em disputas eleitorais, mas que há, sim, novidades em todas as eleições. Então, eu sei o que foi a última eleição, eu sei o que foi a penúltima eleição, mas eu não sei o que será a próxima eleição. E, ao legislarmos apontando para trás, olhando pelo retrovisor, é pouco provável que nós alcancemos uma eficácia dos objetivos que desejamos, porque quem age maliciosamente, quem busca, de modo artificial, interferir numa dinâmica política buscará caminhos. Também muita

gente que não tem um compromisso ético e é capaz de manejar informações, apesar de oferecer risco à saúde das pessoas — que é o que se vê hoje, no caso da vacina —, manejará isso de modo criativo, para usar uma expressão talvez leve. Portanto, eu não tenho qualquer ilusão com relação a uma solução mágica.

Agora, acredito que nós precisaríamos ter uma referência forte. O Prof. Danilo Doneda levantou isso de outro ângulo, assim como a Dra. Jaqueline Abreu, que fala que deveríamos aperfeiçoar os caminhos feitos hoje na norma. Talvez aqui ela versasse sobre Direito Penal, que foi uma questão apresentada a ela, do que propriamente sobre a legislação de privacidade.

Mas eu queria resgatar essa ideia do Prof. Danilo Doneda de que nós deveríamos pensar no desenvolvimento da Lei Geral de Proteção de Dados Pessoais, na sua aplicação, de modo a que possamos realizar a proteção à privacidade, o que não é uma coisa muito simples.

Mas eu queria partilhar com vocês, para concluir, os meus medos, sobre o quais já debati com o João Brant mais de uma vez. Ele fala de três hipóteses: não fazer nada, digamos assim; manter o art. 10; e modificar ou aperfeiçoar o art. 10. Eu confio muito no João e confio muito no Prof. Pablo Ortellado, que é um interlocutor importante sobre essa matéria, pelo profundo compromisso ético e democrático profundo que eles têm. Mas confesso que temo pelo vigilantismo e queria que o João pudesse trabalhar um pouco mais isso e quem quiser falasse sobre isso.

Eu temo pelo vigilantismo que podemos instituir a partir das regras de rastreabilidade, digamos assim, porque temo pela eficiência. Em que medida a quebra da cadeia de encaminhamento e reencaminhamento poderia, digamos assim, fragilizar essa busca que nós temos de trabalhar o art. 10, João? Essa é uma primeira dúvida.

Hoje em dia, eu falo por mim, é muito comum eu fazer uma postagem no Twitter e colocá-la no meu Instagram, digamos assim. Eu, graças a Deus, sei trabalhar a informação. Mas é muito fácil trabalhar em plataformas diferentes. E a minha dúvida é se isso não ajuda a quebrar e limita a chegar aonde nós queremos chegar.

A Bruna levantou uma preocupação que ela tem, que eu acho relevante, sobre o encaminhamento de informações e o risco que pode oferecer tal artifício. Muita gente faz, junta, mobiliza. Vejam agora dia 7 de setembro, eu acho um horror a pauta que está sendo provocada pelo campo conservador. Eu acho um horror! Mas se for dentro das regras, digamos assim, do jogo... Eu temo pela eficiência e pelos riscos que poderia trazer e queria que o João falasse um pouco sobre isso.

Aparece ali, João, também, a questão da quebra da criptografia, se pudesse também falar sobre isso valeria a pena. E uma hipótese que eu cheguei a pensar sobre a guarda até de metadados era se nós pudéssemos fazê-lo apenas na hipótese de se atender demandas de produção de provas de uma investigação criminal. Seria *a posteriori*, digamos assim, ou seria por instrução de um determinado processo. Se alguém quiser falar algo, isso é parte da reflexão que nós deveríamos fazer.

De uma coisa eu estou seguro: aos críticos do art. 10, do PL nº 2.630, eu diria que a mera crítica ao art. 10 talvez seja insuficiente, porque não se pode ter aquela atitude imortalizada numa expressão famosa do Caetano Veloso, aquela história que é tão falada: "*Eu sei o que eu não quero, mas eu não sei o que eu quero*". Nós precisávamos dar um passo adiante antes. Se for fazer o debate do art. 10 do PL nº 2.630, precisaríamos partir de um diagnóstico. É uma ação maliciosa responder: o que fazer para combatê-la?

Não sei se me fiz entender. Foi uma provocação que não é dirigida. Eu falei muito do João Brant porque, digamos assim, foi uma voz dissidente na mesa, uma voz mais peculiar. Mas são questionamentos que estão abertos para reflexão de todos vocês.

Como sempre faço nas audiências públicas, queria que todos tivessem a porta aberta para oferecer sugestões de textos, de análise, de documentos, sugestões de texto legal para que possamos incorporar no relatório final desse grupo de trabalho.

Muito obrigado pela participação de todos.

Muito obrigado pela condução, querida Presidente Bruna Furlan.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Eu que agradeço. É muito bom trabalhar com V.Exa. Embora em campos opostos da política, nós temos muitos pontos de convergência, como gostar muito dessas audiências pública, de ouvir as pessoas, ouvir tudo que elas têm para compartilhar conosco, pelos seus ensinamentos, pelo tanto que sabem.

Essas audiências para nós, eu posso falar por mim, mas acho que por V.Exa. também, é a melhor parte do trabalho.

Eu quero também cumprimentar a Deputada Angela Amin.

Eu passarei a palavra ao nosso Deputado Gustavo Fruet, pelo tempo que quiser, e aos demais Parlamentares. É importante ouvirmos o Deputado Rui Falcão, por um minutinho. Eu sei que ele está atento ouvindo todas as exposições. É importante ainda a Deputada Lídice da Mata falar, assim como todos os Parlamentares.

Concedo a palavra ao Deputado Gustavo Fruet.

O SR. GUSTAVO FRUET (PDT - PR) - Presidente Bruna Furlan, é um privilégio revê-la. Hoje eu estou matando a saudade de vir à Comissão acompanhar mais uma audiência muito qualificada.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Muito obrigada.

O SR. GUSTAVO FRUET (PDT - PR) - Cumprimento todos os palestrantes, a Deputada Angela Amin, o Deputado Relator Orlando Silva, que já apresentou o ponto principal desta audiência. Ao cumprimentá-los, registro o agradecimento ao Danilo, à Jaqueline, à Miriam, à Bruna, à Samara e ao João Brant.

Abordareis dois pontos. Primeiro, é um ponto comum, que trata da preocupação em identificar agentes maliciosos, sem ferir princípios, direitos, em especial constantes na LGPD. Isso parece ser evidentemente um consenso. Segundo, é um desafio do Relator ao desenhar uma arquitetura: como estabelecer mecanismos de combate, sem ferir os princípios já mencionados?

Eu tive o privilégio de ter dois professores de Direito Penal, René Dotti e Luiz Alberto Machado, que sempre questionaram muito o excesso legislativo e a tendência de imaginarmos que toda mudança geracional, ciclos e, principalmente, tecnológica, exige uma legislação especial. Nós mal nos acostumamos a consolidar determinados documentos legislativos e sempre estamos partindo para a elaboração de novos documentos legislativos. É inevitável que se gere conflito entre quem elabora a lei, quem a aplica e a quem ela é dirigida. Em muitos momentos esse conflito, esse embate acaba sendo muito sutil e gera evidentemente um eterno questionamento.

Nesse caso específico, nós estamos mais uma vez pensando de forma ortodoxa em um tema que tem uma agilidade de transformação e mudança que, por mais que acompanhemos as mudanças legislativas, em qualquer país, em especial no Brasil, sempre há a impressão de que estamos atrasados e se gera o risco de estabelecer restrições, mesmo que se vise com boa-fé ao combate a determinados desvios.

Eu acho que o desafio do Relator é estabelecer como se dará esse combate, se será pelos mecanismos tradicionais, no caso do Poder Judiciário, ou com medidas novas que gerem embate, dando mais poder e cobrança às plataformas com relação à moderação.

É uma observação para o Relator. O ponto principal, hoje, além da reflexão — eu peço a manifestação final aos convidados, cumprimentando-os pela qualidade — é em relação às propostas da alteração do art. 10. Efetivamente temos algo objetivo sendo trabalhado e seguramente será um ponto que o Relator poderá acolher e apresentar alguma modificação.

Presidente, mais uma vez, muito obrigado, e parabéns pela qualidade desta audiência!

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Muito obrigada, Deputado Gustavo Fruet.

Vê-lo aí me dá saudades desse plenário. Tantas vezes nós estivemos aí, mas a nova realidade nos fez nos adaptarmos ao sistema híbrido.

É muito bom vê-lo. Muito obrigada, pelas suas palavras.

Katia, há mais algum Parlamentar inscrito?

A SRA. KATIA DA CONSOLAÇÃO DOS SANTOS - Sim. Há a Deputada Lídice da Mata.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Tem a palavra a Deputada Lídice da Mata.

A SRA. LÍDICE DA MATA (PSB - BA) - Bom dia!

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Bom dia!

A SRA. LÍDICE DA MATA (PSB - BA) - Quero saudar a Presidente Deputada Bruna Furlan, todos os companheiros Deputados presentes nesta reunião, no plenário ou virtualmente, e os grandes especialistas que estão conosco, nesta reunião, neste debate. A Deputada Angela Amin *(falha na transmissão)*.

Esse debate sobre o art. 10 encerra praticamente a discussão central do nosso dilema, inclusive, da implantação da CPMI da Fake News, que responde a um clamor da política e da sociedade de como combater a desinformação, *fake news*, etc.

Se é verdade que há uma um excesso legislativo — e eu compreendo isso, sem dúvida —, por outro lado, nós precisamos, como o próprio Deputado Orlando Silva disse, investigar, ir a fundo nesta discussão, para ver até onde podemos ou não podemos ou não devemos agir, numa determinada direção. Está claro, hoje, consolidado, que não existe a chamada bala de prata para resolver essa questão. Nós teremos que atuar em diversas linhas, em diversas direções. Eu sinto certa necessidade de darmos resposta à angústia de todos, porque sempre que eu debati com especialistas, nesse período, Deputada Bruna Furlan, sempre fica uma dúvida. Muitos companheiros dizem: *"A legislação já existe, não é preciso fazer mais nada"*.

Se ela existe, teria a capacidade, a eficácia de coibir a existência da prática do crime. Essa não é uma verdade absoluta, porque a legislação penal que produz uma legislação, que pune determinados crimes, não impede que eles ocorram.

É preciso, quando se discute a legislação, discuti-la dentro de determinados parâmetros. Eu não sou advogada, muito menos criminalista, mas tenho a minha experiência legislativa. Afirmar, por exemplo, que nós só fazemos uma legislação posterior ao crime, isso é geralmente o que acontece. Quando há determinado crime, há um clamor popular em relação a ele e a Câmara dos Deputados se volta para discutir como vai classificar, penalizar e punir a sua prática. Tudo isso envolve, portanto, questões com muita relatividade.

Eu gostei pessoalmente de todas as falas que buscaram caracterizar, principalmente, a necessidade da manutenção da defesa da Lei Geral de Proteção de Dados Pessoais, da proteção dos usuários, mas eu creio que o João Brant apresentou um aspecto que me parece muito importante, que é demonstrar que existe, efetivamente no Brasil e em algumas outras sociedades, um impacto extremamente negativo na formação de opinião pública via WhatsApp, e nós não podemos ignorar este fato.

Quando se trata de política, a nossa tendência, da sociedade em geral, digamos, dos não "políticos profissionais", entre aspas, é dizer que isso é problema da política. Foi assim inclusive no início do debate da CPMI da Fake News, como se uma parte da sociedade, inclusive a imprensa, dissesse que isso é problema da política, que está tentando discutir o terceiro turno eleitoral, não vamos nos meter nisso.

Mas aí veio a pandemia e, com ela, veio o impacto desse tipo de prática, que eu creio, em determinado momento, criminosa, sobre o conjunto da sociedade implicando e impactando inclusive na proteção da vida propriamente dita. E isso faz com que tenhamos uma nova experiência no tratar dessa questão.

Então, eu ouvi com muito interesse a sugestão que ele apresentou aqui de tentativa até de sair daquela discussão se vamos empoderar as redes sociais, as plataformas, ou vamos empoderar algum mecanismo de censura no Brasil etc., quando ele coloca: *"Vamos empoderar o usuário"*. Esse é o conceito maior, e nós deveríamos investigar mais como tratar isso.

É claro que essa angústia nossa não se resumirá numa lei draconiana contra *fake news*, que não terá eficácia e que irá enrijecer a liberdade na rede. Mas a própria rede vai encontrando mecanismos de autodefesa. Uma característica disso é justamente o Sleeping Giants, que consegue fazer numa campanha a denúncia de determinadas empresas que, sem querer ou querendo, financiam redes e pessoas relacionadas à prática reiterada de *fake news*.

Está comprovado também, tanto pelas investigações do Supremo Tribunal quanto pelas nossas investigações na CPMI, que havia uma prática organizada e com financiadores, portanto, caracterizando uma espécie de quadrilha em ação em determinado momento. E na questão das *fake news* voltadas para a pandemia, isso também se relacionava.

Portanto, é claro que essa prática leva-nos a debater algum nível de legislação criminal. Acho que não deve ser essa a ênfase da nossa discussão e do nosso trabalho. O desafio não é só nosso, o desafio é mundial. Muitos estão tentando. Isso tudo demonstra que muitos estão tentando porque há um claro dano à sociedade a existência dessa prática. De forma mais destacada, algumas sociedades, como no Brasil e na Índia, muito populosas, demonstram também falta de informação geral da população. Através do WhatsApp, que é um mecanismo privado, em que a notícia não está aberta a todos, não há um "controle", entre aspas, da formação de opinião como reação, porque se leva tempo, pelo menos algum tempo, para descobrir que aquela notícia ou aquela desinformação está rolando. Por isso, essa plataforma se transformou na predileta para a prática de determinados crimes. Durante a pandemia, foram crimes contra a vida das pessoas. Hoje está sendo, porque nós não saímos da pandemia. Eu não estou discutindo apenas essa circunstância, que o Orlando retratou muito bem, da mobilização agressiva para o 7 de Setembro. Ela responde a determinado pensamento existente na sociedade. Nós podemos dizer que é livre a manifestação de organização no País, dentro dos limites da Constituição Federal. Mas isso é diferente da mobilização feita para dizer, por exemplo, que os caixões estavam vazios, que não existia uma pandemia letal com capacidade intensa de combater todas as medidas preventivas de isolamento, de máscara etc., com negação do funcionamento da ciência.

Vejam que são desafios novos também. Da mesma forma que nós estamos lidando com a tecnologia nova, essa tecnologia incide sobre comportamentos nocivos da vida em sociedade. Novos, porque a mentira existe há muito tempo, desde que a humanidade existe. Todos reafirmam isso. A prática da mentira na política, da calúnia, etc. também existe desde que a política existe. Mas, com determinada evolução dos meios e das ferramentas de comunicação na sociedade, elas passaram a ter outro tipo de prejuízo à vida dessas pessoas. Algumas, inclusive, perderam sua própria vida, expostas a determinado tipo de campanha nociva. Então, eu estou dizendo isso porque sei do bom senso, do senso comum, do politicamente correto. Eu não tenho dúvida da afirmação da liberdade de expressão, da necessidade da preservação de dados. Mas nós temos que encontrar caminhos. O Orlando, por exemplo, indicou certa quebra de criptografia, no caso de se caminhar para a necessidade de formação de provas de determinado crime.

Veja bem, quando se discute isso, está-se relativizando, de alguma maneira, essa liberdade. Se a criptografia existe para manter a privacidade, ela pode ser quebrada no momento em que isso signifique ameaça à vida de determinadas pessoas. Então, eu creio que nós precisamos discutir esse assunto em outro lugar que não é o de vocês, como especialistas e pesquisadores, mas no lugar da representação da sociedade, de como a sociedade é atingida, de como ela se sente impotente diante desses movimentos. Assim, acho que devemos todos buscar pontos comuns e abrir as mentes, tanto nós quanto todos os pesquisadores, para encontrarmos caminhos. Que, de alguma maneira, tenhamos mecanismos que possam inibir isso.

Eu volto a dizer: nada impede o cometimento de crime. A legislação mais dura, que é a pena de morte, não impede que os crimes previstos com pena de morte sejam cometidos no mundo e nas sociedades onde elas estão legalizadas, onde esta prática é legalizada. No nosso País não existe pena de morte formal. Mas existe para alguns. Mesmo assim, é necessário um ambiente de vida em sociedade em que nós possamos encontrar mecanismos que indiquem a punição em determinado grau, de determinada forma, para determinados crimes.

Por isso, eu sou simpática tanto a essa proposição do Deputado Orlando, quanto àquele caminho que João Brant indicou e a outros caminhos que busquem uma transparência grande na rede. Eu sempre defendi que o direito à informação era um direito do cidadão brasileiro, bem como o direito a informar, antes de haver esse tipo de mecanismo de rede social. Eu acho que ser informado é um direito do usuário, e também de onde ele recebe determinada notícia. É um direito do usuário perceber se ele está sendo vítima de um golpe, de como esse golpe está ocorrendo. Outros mecanismos de crimes estão ocorrendo na rede, diversos. Todos os dias nós estamos recebendo notícias, até nas redes dos Deputados, que estão sendo clonados e estão pedindo dinheiro. Tenho muitas pessoas amigas que ligam para dizer que foram vítimas de crime partido da Internet.

Então, precisamos discutir não apenas o PL 2.630, mas partir do princípio de que a rede também é um lugar em que hoje ocorrem crimes de diversas naturezas. Que possamos levar isso em conta no debate. Senão fica parecendo, em determinado momento... Desculpem-me a franqueza, vocês podem até julgar que é uma posição *démodé*, mas algumas horas eu fico me perguntando para que estamos discutindo se tudo está previsto, se nada pode ser feito, se tudo que nós fizermos, de alguma forma, invade a liberdade de expressão, que eu sempre defendi, minha vida inteira, como indispensável.

Então, é preciso nos abrir para discutir alguns caminhos, e eu acho que João Brant tentou fazer isso neste momento, não sei se do modo mais eficaz, mas creio que partiu de algo determinado da sua própria pesquisa: 70% ou 80% da formação de opinião no Brasil está vindo do WhatsApp e da desinformação. Ele colocou um dado muito importante: uma boa parte ou a maioria dos usuários hoje desconfia da notícia que vem do WhatsApp. Então, nós entramos numa outra coisa, que é o mecanismo de desconstrução de imagem, de determinada forma como ela se apresenta. E eu acho que esse é o dado mais positivo que vi recentemente, porque, no início dessa discussão, há 1 ano e meio ou 2 anos, o WhatsApp era a grande forma de comunicação, e de grande credibilidade. Se nós conseguimos, até então, com esse debate, começar a descredibilizar as mensagens que vêm daí, começamos a ter vitórias. E não foi preciso haver empresa de checagem; foi preciso principalmente haver o debate intenso na sociedade e, talvez, a sociedade ter vivido o que viveu, infelizmente, e ainda vive hoje, com a pandemia.

Eu sei que falei demais, e talvez tenha colocado algumas posições não muito claramente. Elas fazem parte da minha angústia de debater esse assunto há 1 ano e meio. Em muitos momentos eu me senti aprisionada como um cachorro correndo atrás do próprio rabo, mas acho que há caminhos. Tenho esperança nesses caminhos, tenho esperança na nossa capacidade de suar o cérebro para produzir algum tipo de resultado, que não será a bala de prata, mas caminhos de estímulo à sociedade "normal", entre aspas, para começar a ter conhecimento a respeito do tema, para começar a se envolver com o tema de tal forma que ela própria comece a gerar sua autoproteção.

Obrigada.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - A Deputada Lídice fez importante reflexão, que já fica aí para os nossos expositores aproveitarem nas suas considerações finais.

Eu também tenho interesse, assim como o Deputado Orlando Silva, em ouvi-los sobre o vigilantismo.

Pergunto à nossa colaboradora Katia se existe mais algum Parlamentar inscrito.

A SRA. KATIA DA CONSOLAÇÃO DOS SANTOS - Não há mais Deputado inscrito.

A Deputada Angela Amin está na sala do Zoom. Talvez fosse bom consultá-la sobre se deseja falar.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Deputada Angela, muito obrigada pela sua participação. Se deseja falar, a palavra está com V.Exa.

A SRA. ANGELA AMIN (PP - SC) - Eu apenas gostaria de cumprimentá-la por mais esta audiência. Acho que o tema demonstra uma preocupação de todos nós. A Deputada Lídice colocou muito bem o assunto, e aprofundar e estudar faz parte do nosso trabalho nesta Casa.

Parabéns a todos os que deram a sua contribuição.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Muito obrigada, Deputada Angela.

Vou passar a palavra aos nossos expositores, para as suas conclusões finais.

Pelo tempo de 3 minutos, passo a palavra ao nosso querido Prof. Danilo Doneda, para suas considerações finais.

O SR. DANILO DONEDA - Muito obrigado, Deputada Bruna Furlan. Agradeço o interesse e a participação direta do Relator Orlando Silva, da Deputada Lídice da Mata, da Deputada Angela Amin, do Deputado Gustavo Fruet, entre outros que tenham participado do debate.

Antes de tudo, fazendo menção aos comentários do Deputado Gustavo Fruet, digo que o Deputado teve a mesma *(ininteligível)* a mesma faculdade que eu fiz, a Universidade Federal do Paraná. Os mestres que ele citou, os Profs. René Ariel Dotti e Luiz Alberto Machado, foram também meus mestres de direito na *(falha na transmissão)* ainda que eu não tenha enveredado para o direito penal, muito pelo contrário. O Prof. René Ariel Dotti, pelo menos, foi o primeiro grande militante da causa da privacidade e da proteção de dados. Seus estudos, seus ensinamentos são a centelha de praticamente tudo isso que nós discutimos hoje, na sua atividade advocatícia, na defesa de liberdades fundamentais, inclusive numa época difícil no nosso País, enfim, a preocupação com a privacidade surgiu para ele como uma necessidade também *(falha na transmissão).*

Desculpem-me, eu acho que a conexão caiu e voltou. Vocês estão me ouvindo?

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Agora, sim.

O SR. DANILO DONEDA - Desculpe-me, Deputada Bruna. Vou tentar retomar — ainda tenho tempo —, indo direto à questão. Vinha falando dos Profs. René Ariel Dotti e Luiz Alberto Machado.

Falando agora diretamente dos comentários em relação ao art. 10 do projeto de lei, daquilo que foi mais tratado, o debate ficou muito concentrado na não existência de uma bala de prata, e, ao mesmo tempo, soluções foram apresentadas como eventuais balas de prata. Muito sucintamente, acredito que os riscos da rastreabilidade *(falha na transmissão).*

A SRA. LÍDICE DA MATA (PSB - BA) - Não estou ouvindo.

O SR. DANILO DONEDA - ...princípio da Lei Geral de Proteção de Dados é muito *(falha na transmissão).*

A SRA. LÍDICE DA MATA (PSB - BA) - A conexão caiu.

Estão ouvindo?

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - O áudio está variando um pouco. Ele fala e o áudio para um pouquinho.

Professor, se puder, por favor, recomeçar para com atenção nós o ouvirmos, retornaremos o tempo de 3 minutos.

O SR. DANILO DONEDA - *(Falha na transmissão)* funcionalização de regras juridicamente entranhadas na LGPD é um problema que deve ser visto com bastante seriedade. A mitigação *(falha na transmissão)* vai afetar pessoas e grupos vulneráveis, certamente. Além do mais *(falha na transmissão).*

Estou com problema, Deputada. Eu prefiro abrir mão do tempo para não prejudicar o decorrer da audiência.

Muito obrigado pela atenção.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Obrigada, Prof. Danilo. Se restabelecer a conexão, avise-nos, para lhe passarmos a palavra depois da fala dos demais expositores.

Eu gostaria de passar a palavra, pelo tempo de 3 minutos, para a Dra. Jacqueline Abreu, pesquisadora e membro da Comissão de Juristas Proteção de Dados Pessoais.

A SRA. JACQUELINE ABREU - Muito obrigada, Deputada. Agradeço também os comentários dos demais Deputados que manifestaram suas preocupações. Eu acredito que todas elas são centrais, principalmente esses comentários feitos na linha do vigilantismo.

Efetivamente, nos moldes como está posto hoje, o art. 10 traz um risco muito forte para a criptografia em si, olhada estritamente, para a proteção de dados, mas também facilitaria a utilização dessa ferramenta para propósitos vigilantistas,

por exemplo, para criminalizar movimentos sociais que são democráticos, ou o trabalho jornalístico, ou até o trabalho político. Eu acredito que esse é um risco efetivamente muito grande. Estamos discutindo até hoje, e há tanto tempo, a desinformação. O PL inclusive abandonou a tentativa de definir o que é isso, sem, é claro, abandonar o projeto acadêmico de estudar esse tema. Mas esse dispositivo ainda ficou, e me parece que ele deve ser abandonado, nessa mesma perspectiva. O dispositivo, tal como hoje está posto, na verdade seria inadequado, e ele traz um risco muito grande para a proteção de dados, além de poder ser mal utilizado.

Os Deputados também comentaram sobre a existência de alternativas. Eu acho, efetivamente, que é isso que devemos buscar.

Como eu comentei, na Comissão de Juristas chegamos a pensar uma redação alternativa que olhe para a preservação prospectiva de registros de interação, sem vinculação com o conteúdo, dentro de uma suspeita de que aquela conta específica está sendo utilizada para algum tipo de conduta criminosa. Essa moldura teórica carrega em si muito mais respeito à proteção de dados pessoais e trabalha noções que já são conhecidas no processo penal, como a proporcionalidade e a existência de uma suspeita individualizada. Por isso ela é interessante.

Ao mesmo tempo, está havendo discussões, por exemplo, sobre o Código de Processo Penal e as alterações que isso representaria. Esse tipo de dispositivo é sobre meio de obtenção de prova, não sobre alteração da legislação penal, porque os crimes vão continuar acontecendo, e uma discussão sobre meio de obtenção de prova deve questionar efetivamente se aquilo vai servir para responsabilizar alguém, para alcançar a prova que se pretende.

Como está posto, o art. 10 é um problema. A alternativa que veio da Comissão deve ser pensada amplamente, como uma proposta que vai afetar o processo penal de forma geral, inclusive a investigação de outros crimes, e que pode trazer outros tipos de preocupação sobre a sua pertinência, por isso deve ter a discussão ampliada.

Parece-me, nessa linha que eu venho seguindo, que nós devemos também amadurecer a discussão sobre a LGPD penal, a Lei Geral de Proteção de Dados aplicada à segurança pública e às investigações criminais, antes de ficar pensando em criação de novos meios de obtenção de prova, ou pelo menos isso deve caminhar paralelamente.

Esse é o recado que eu deixaria nesta minha observação final.

Muito obrigada, mais uma vez, pelo convite.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Dra. Jaqueline, muito obrigada pelas suas considerações finais.

Eu gostaria de passar a palavra para a Miriam Wimmer, Diretora da Autoridade Nacional de Proteção de Dados, para suas considerações finais.

Eu tive que desligar o vídeo, mas estou atenta a tudo.

A SRA. MIRIAM WIMMER - Pois não, Deputada. Muito obrigada. Eu queria agradecer os seus comentários e os relevantes questionamentos da senhora e dos demais Deputados e Deputadas.

Vou começar estas considerações finais ressaltando que me parece que a desinformação é, sim, um problema muito relevante. Quando diversos especialistas falam da importância de se levarem em consideração aspectos ligados à proteção de dados e à privacidade, isso de forma alguma diminui a relevância que se atribui a esse grave problema.

Eu ouvi muito atentamente a Deputada Lídice falar da angústia que ela sente por esse fenômeno. Eu concordaria com a avaliação dela de que esse não é um fenômeno que se restringe à classe política, mas afeta profundamente toda a sociedade. Esse enfraquecimento dos espaços de debate público, esses problemas de polarização, esses problemas de risco à saúde e à vida são de fato muito relevantes, e me parece muito salutar e muito louvável que nos debrucemos sobre estratégias de enfrentamento a esse problema.

Por outro lado, parece-me importante salientar, mais uma vez, como já dito, que as nossas abordagens devem ser múltiplas. Várias estratégias regulatórias devem ser buscadas, que envolvam aspectos de educação, aspectos de tecnologia, aspectos relacionados aos modelos de negócios, incentivos financeiros, aspectos ligados à transparência. Achei muito interessante a Deputada Lídice mencionar que a própria rede vai encontrando mecanismos de defesa. Ouvindo essa fala, eu me pego pensando que de fato nós temos hoje um problema associado a um modelo de negócio específico: a mensageria instantânea. Mas quem sabe o que acontecerá nas próximas eleições? Porque a tecnologia se altera muito rapidamente, e as formas de comunicação no espaço público também sofrem essas alterações.

Acho que é pertinente lembrar a fala do Deputado Gustavo Fruet sobre essa combinação de mecanismos públicos e privados. Nós temos hoje um regime jurídico que envolve tanto moderação privada de conteúdo quanto atuação pelo próprio Poder Judiciário. E o papel da ANPD, como eu mencionei, não se volta a analisar conteúdo de mensagem, mas sim a promover um fluxo mais adequado de dados pessoais. Nesse sentido, acho importante frisar, fazendo um contraponto a uma das falas, que os dados publicamente disponíveis são também protegidos pela LGPD, na medida em

que reconhecemos o dado pessoal como uma projeção da personalidade humana, um direito fundamental autônomo. Entende-se que esses princípios de finalidade, adequação, necessidade devem ser observados em todos os espaços públicos e privados de comunicação, porque estamos falando essencialmente de um direito associado à personalidade humana. A nossa legislação já possui algumas normas que obrigam a guarda de metadados, como o Marco Civil da Internet. E me parece que aqui, enquanto discutimos novas obrigações de guarda de metadados, fazer essa avaliação cautelosa e proporcional de fato é necessário, tendo em vista também os riscos que são provocados.

Muito obrigada mais uma vez.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Dra. Miriam, muito obrigada pela sua importante participação em nossa audiência pública.

Eu gostaria de passar a palavra, para suas considerações finais, à Bruna Martins dos Santos, representante da Data Privacy Brasil.

A SRA. BRUNA MARTINS DOS SANTOS - Obrigada, Deputada. Também agradeço os comentários do Deputado Orlando, da Deputada Lídice, do Deputado Gustavo Fruet e da Deputada Angela Amin.

Na minha opinião, o grande debate sobre o art. 10, já partindo para ele diretamente, é justamente como chegar à solução de uma medida adicional de investigação exclusivamente dedicada à disseminação da desinformação sem minar essa ferramenta fundamental para o sigilo e a não intervenção em nossas comunicações que é a criptografia. Até o momento, boa parte das soluções que nós discutimos, ou que têm sido aplicadas pelo mundo, se demonstram ineficazes, por exemplo, por essa questão que eu comentei mais cedo sobre o conjunto de informações, ou a informação falsa em si, não existir exclusivamente numa plataforma. Isso torna muito difícil identificar os autores do conteúdo.

Sobre a criptografia, eu queria dizer que não existe quebra parcial de criptografia, não existe meia quebra, ou quebra de um pedacinho dela. Nesse cenário, empoderar o usuário é garantir o seu direito a uma proteção de dados e à proteção das suas comunicações. A rastreabilidade, da maneira como está colocada, ela afeta, sim, a criptografia, a segurança e as comunicações de um grupo grande de jornalistas, de ativistas, de pessoas comuns, e ignora que a criptografia é esse recurso que protege a segurança das nossas comunicações, o que é fundamental paras as nossas interações digitais.

Para falar um pouco mais da rastreabilidade, eu diria que ela em si é um conceito até regulatório, que pode ser implementado, por exemplo, por coleta de metadados, por quebra de criptografia, e que a coleta de metadados em si também permite uma relativização da proteção de comunicações realizadas, por exemplo, com a criação de mapas de interações de atores políticos. E, por mais bem-intencionados que estejamos em relação ao PL 2.630, eu me preocupo muito com o eventual abuso desse mecanismo de rastreabilidade, identificação, coleta de metadados, especialmente por um Governo que tem contratado, cada vez mais, tecnologias que violam a nossa privacidade, tecnologias de vigilância massiva, que vão gerar, no fim do dia, esse processo de criação de dossiês, intimidação de indivíduos, que é chamado de *chilling effect*, reconhecido, pelo próprio Supremo Tribunal Federal, como um processo problemático, porque limita a liberdade de expressão e deixa todo mundo muito receoso com relação ao que pode falar, a como se pronunciar, a em que momentos pode professar suas opiniões num ambiente autoritário. Então, eu tenho medo, ainda mais ante a escalada autoritária que o País tem enfrentado — do que vai ser feito com as cadeias de mensagem, com os nossos metadados, com os *links* que são enviados, por exemplo, em grupos de partidos políticos, num cenário em que não temos mais controle da nossa democracia, em que o controle é cada vez mais retirado.

Para terminar, se fôssemos pensar em alguma via para o art. 10, considerando que esses regimes de retenção de dados são, sim, interferências relevantes sobre uma série de direitos e liberdades fundamentais, a política legislativa deveria evoluir de maneira extensamente justificada e articulada, para que ela não seja desproporcional, e deveríamos pensar em casos específicos, não numa medida genérica aplicada a todos os usuários da rede.

Essa é a minha fala.

Muito obrigada, Deputada Bruna.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Eu é que agradeço, xará. Muito obrigada.

Eu gostaria de passar a palavra, pelo tempo de 3 minutos, para as considerações finais, à Dra. Samara Castro, membro do Instituto Nacional de Proteção de Dados e Vice-Presidente da Comissão de Proteção de Dados da OAB do Rio de Janeiro.

Com a palavra a Dra. Samara.

A SRA. SAMARA CASTRO - Obrigada, Deputada.

Quero agradecer a todas as Deputadas e a todos os Deputados presentes, que possibilitaram este debate tão interessante.

Agradeço também aos meus companheiros e companheiras de Mesa, a quem eu admiro bastante.

É sempre bom falar desse tema da rastreabilidade, porque eu sei que é o que aquece mesmo o debate.

Eu tenho mais concordância com o que o João colocou. Sei que é a parte polêmica, mas acho que é importantíssimo que façamos essa discussão do que são as comunicações dentro dos aplicativos de mensageria privada, do que são as comunicações privadas e do que são as comunicações massivas. Nem tudo o que está dentro dos aplicativos de mensageria privada merece e precisa da proteção da privacidade, da mesma proteção que a comunicação privada necessita. Então, acho que fazer essa diferenciação é fundamental.

Acho que um dos critérios — eu já tinha colocado como sugestão, mas reforço — é a porta de entrada. A porta de entrada, sendo pública, já demonstra que aquele espaço tem mais requisitos para ser um espaço público e não um espaço privado. Então, os grupos que têm *links* públicos, os grupos que circulam de forma pública, na minha opinião, deveriam ter uma proteção mitigada em relação aos grupos que são estritamente privados, estritamente relacionados à vida privada, que realmente deveriam ser protegidos dessa forma.

A proposta que o João colocou está bem interessante. Ela avança em vários aspectos que nós já temos debatido há um tempo. Acho inclusive que ela contribui para o que são essas preocupações no sentido anterior da rastreabilidade. Então, a minha compreensão é a de que realmente avancemos a partir dali. Eu daria a sugestão de incorporarmos não como critério adicional dentro da proposta, mas como critério autônomo a questão da porta de entrada dos grupos de *link*s públicos para que realmente eles sejam considerados como mais passíveis de mitigação. Além disso, acho que nessa proposta deve ser pensada a possibilidade de oferecer ao usuário o critério de poder a mensagem ser encaminhada ou não, da mesma forma que o Facebook hoje dá a possibilidade de se colocar para encaminhar a amigos, a todo mundo, a amigos de amigos. Enfim, é colocar a mensagem assim. Acho que, dessa forma, conseguiremos avançar bastante.

É isso.

Muito obrigada.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Samara, muito obrigada pelas suas considerações finais.

Eu gostaria de passar a palavra para o Prof. Dr. João Brant, Diretor do Instituto Cultura e Democracia.

O SR. JOÃO BRANT - Obrigado, Deputada Bruna Furlan e todos os Deputados presentes.

Eu vou responder diretamente algumas questões do Deputado Orlando, aproveitando os meus 3 minutos para isso, e dialogar também com algumas falas que me antecederam.

É muito essencial que busquemos conciliar a maior proteção de dados possível com o enfrentamento à desinformação. Essa tarefa não é pequena. Essa tarefa é enorme. Ela nos exige energia e disposição para buscar soluções. Acho que a questão-chave, repito, para mim, é como separamos o que é comunicação privada do que é comunicação de ordem pública.

De toda forma, eu queria falar três coisas.

Da maneira como essa proposta está no art. 10, muito menos nos termos que eu propus, não há quebra de criptografia. Podemos discutir os efeitos disso numa possível identificação e associação à pessoa e ao conteúdo — acho que esse é um debate aberto para ser feito —, mas há um debate internacional sobre isso, sobre se há ou não quebra de criptografia. Há posições defensáveis dos dois lados. Acho que não há quebra de criptografia. O próprio WhatsApp, ao fazer isso nos conteúdos multimídia de usar *hashs* de referência e usar essa dimensão de *hash* para compartilhamento, já nos aponta um caminho.

Deputado Orlando, acho até que a possibilidade de utilizar uma rastreabilidade dos arquivos multimídia, nos termos que o WhatsApp já faz, talvez seja um dos caminhos possíveis também para se mitigar os riscos.

Sobre o vigilantismo — se eu acho que há risco —, sem dúvida, há riscos, e temos que olhar para eles. O problema é que temos riscos eventuais de um lado e temos danos certos do outro. Então, a existência de riscos não deve nos parar. Ela deve nos provocar positivamente para olharmos e entendermos como podemos mitigar esses riscos e diminui-los ao máximo. Se a proposta hoje é considerada desequilibrada por um segmento grande da sociedade civil, é muito positivo que busquemos soluções de aprimoramento e, de fato, apontemos numa direção que não vá só lidar com questões *a posteriori*. Acho que isso é muito claro. O próprio Marco Civil, não é à toa, prevê a retenção de dados no sentido de acesso a aplicações *a priori*. Sabemos que *a posteriori* lida-se com problemas específicos e casos muito específicos de investigação. Do meu ponto de vista, não basta lidar com o problema *a posteriori*.

É importante dizer também da eficiência da proposta. Qualquer proposta vai ter fragilidades, e nós precisamos também botá-las na mesa. Acho que isso está sendo feito, mas precisamos entender que a oposição a propostas que são mais ou menos eficientes não pode ser não fazer nada. Então, precisamos buscar propostas que sejam mais eficientes e mais eficazes e consigam, de fato, lidar com o problema com o tamanho que ele tem.

De novo, só faço uma última observação: é essencial fazer um esforço grande para conciliar a proteção de dados com o enfrentamento à desinformação. Acho que isso precisa ser feito a partir da nossa abertura, assim como sentar junto em torno de propostas de caminhos possíveis.

A SRA. PRESIDENTE (Bruna Furlan. PSDB - SP) - Muito obrigada.

Obrigada a todos os que participaram.

Nada mais havendo a tratar, convoco reunião extraordinária para quinta-feira, dia 26 de agosto, às 14 horas, para a realização de audiência pública, conforme pauta a ser divulgada oportunamente.

Está encerrada a nossa audiência.

Agradeço, mais uma vez, a participação de todos. Espero que fiquem todos bem.

Um grande abraço.

QUARTO SEM ÁUDIO