



DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

Versão para registro histórico

Não passível de alteração

CPI - CRIMES CIBERNÉTICOS			
EVENTO: Audiência Pública	REUNIÃO Nº: 2022/15	DATA: 13/10/2015	
LOCAL: Plenário 9 das Comissões	INÍCIO: 15h19min	TÉRMINO: 17h59min	PÁGINAS: 57

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

PABLO XIMENES - Diretor de Segurança da Informação da Empresa de Tecnologia da Informação do Ceará — ETICE.
PEDRO MIZUKAMI - Professor do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas — FGV.
PEDRO MARKUN - Hacker do espaço LabHacker e da comunidade Transparência Hacker.
PEDRO REZENDE - Professor de Ciência da Computação da Universidade de Brasília — UnB.

SUMÁRIO

Investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste País.

OBSERVAÇÕES

Houve exibição de imagens.



O SR. PRESIDENTE (Deputado Rodrigo Martins) - Boa tarde senhoras e senhores!

Declaro aberta a 21ª Reunião Ordinária da Comissão Parlamentar de Inquérito que investiga os crimes cibernéticos.

Encontra-se à disposição dos Srs. membros a cópia da ata da 18ª Reunião, realizada no dia 5 de outubro, em Natal, Rio Grande do Norte.

O SR. DEPUTADO SANDRO ALEX - Peço a dispensa da leitura da ata, Sr. Presidente.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Fica dispensada a leitura da ata, a pedido do Deputado Sandro Alex.

Coloco em discussão a ata da 18ª Reunião.

Não havendo quem queira discuti-la, coloco-a em votação.

Os Deputados que concordam com a ata permaneçam como estão. *(Pausa.)*

Aprovada a ata.

A Ordem do Dia de hoje prevê a realização de audiência pública proposta pelo Requerimento nº 34, de 2015, de autoria do Deputado Leo de Brito; pelo Requerimento nº 56, de 2015, dos Deputados Rogério Peninha Mendonça e Leo de Brito, e também pelo Requerimento nº 60, de 2015, do Deputado Odorico Monteiro.

A audiência trata de segurança na rede.

Convido para compor a nossa Mesa de honra o Sr. Pablo Ximenes, Diretor de Segurança da Informação da Empresa de Tecnologia da Informação do Ceará; o Sr. Pedro Mizukami, Professor do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas — FGV; o Sr. Pedro Rezende, Professor de Ciência da Computação da Universidade de Brasília; o Sr. Pedro Markun, *hacker* do LabHacker e do Transparência Hacker.

Informo a todos que cada convidado dispõe de até 20 minutos para sua exposição. Após as apresentações, será passada a palavra ao Relator, aos Sub-Relatores e aos autores dos requerimentos que propuseram esta audiência pública. Os convidados responderão às indagações e, depois, passaremos às intervenções dos demais Deputados.



Dando sequência, eu convido para fazer uso da palavra o Sr. Pablo Ximenes, Diretor de Segurança da Informação da Empresa de Tecnologia da Informação do Ceará.

Sr. Pablo, V.Sa. dispõe de até 20 minutos. O cronômetro fica localizado à esquerda. Pode usar o microfone sem fio. Se tiver alguma apresentação, pode fazê-la.

O SR. PABLO XIMENES - Tenho.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Fique bem à vontade.

O SR. PABLO XIMENES - Muito obrigado.

Primeiramente, quero desejar uma boa tarde a todos Deputados membros da Comissão, nas figuras do Deputado Rodrigo Martins, do Deputado Leo de Brito e do Deputado Odorico Monteiro, um cearense bom de luta; a todos os membros da Mesa, na figura do Prof. Pedro Rezende; a todos os meus colegas aqui; na verdade, a todos os Pedros.

Esta é uma Mesa de Pedros. Aliás, eu sou a única ovelha negra desta Mesa de Pedros.

O SR. DEPUTADO ODORICO MONTEIRO - Pedro e Pablo.

O SR. PABLO XIMENES - Pedro e Pablo, é verdade.

A contribuição que eu venho trazer para esta Comissão é uma visão um pouco mais desmistificada do que são os dados usados como referência para a tomada de decisões sobre políticas públicas, que são as pesquisas em que muitas vezes nós nos pautamos para fazer a nossa análise do que vale a pena para sociedade. Muitas vezes, essas pesquisas trazem uma visão do prejuízo que determinada conduta traz para a sociedade, e essa conduta, quando o prejuízo é significativo, merece uma atenção do Legislativo. Toda lei vai trazer bônus e ônus, toda ação parlamentar vai trazer bônus e ônus, toda interferência na sociedade vai trazer bônus e ônus, e é preciso o que chamamos de segurança da informação de uma análise de risco, para ver o impacto e o custo das ações e dos riscos aos quais nós estamos expostos, para que as decisões sejam pautadas no que é melhor para a sociedade. Por isso, vamos ver um pouco dessa lógica por detrás das pesquisas que nos subsidiam com dados, principalmente dados financeiros, do que é o prejuízo causado pelo crime cibernético.



Vou começar com alguns dados, só para entendermos esse problema que pode estar por detrás desses dados que nos subsidiam. Vou citar o exemplo de uma pesquisa de 1983, feita pelo FED, sobre as finanças dos consumidores americanos.

Essa pesquisa inflou, erroneamente, as estimativas de riqueza das famílias americanas em 1 trilhão — Deputados, 1 trilhão! —, um erro de 10% na estimativa. Por que um erro como esse acontece com uma instituição como essa, em uma coisa tão séria, que vai definir várias políticas públicas? Pasmem V.Exas., esse erro foi resultado de uma única resposta incorreta de uma única pessoa. Como é que pode somente uma resposta de uma só pessoa causar esse prejuízo para uma sociedade desse tamanho? Essas pesquisas possuem certa sensibilidade, não é?

Aqui embaixo está a referência. Depois, os eslaides vão estar disponíveis.

Outro exemplo disso: em outra pesquisa feita, também, por um órgão americano, o Federal Trade Commission, sobre roubo de identidade — um assunto já mais ligado a crime cibernético —, duas respostas, isoladamente, se adicionadas à pesquisa como um todo, representariam uma variação da estimativa para mais de 37 bilhões. Ou seja, a estimativa que era “x” passaria a “x” mais 37 bilhões, caso as respostas fossem computadas. A adição dessas respostas no cômputo multiplicaria todo o resultado final por três. Duas respostas que fogem da moda — “moda” no sentido estatístico, o valor mais comum — acabam tendo um impacto grotesco no resultado dessa estimativa. Mas, poxa vida, por que isso ocorre? Nós vamos entender por que nem toda pesquisa é igual, nem sempre pode ser encarada da mesma maneira.

Essa pesquisa, em particular, é interessante. Na verdade, não se trata de uma pesquisa, são várias pesquisas. Em um estudo publicado na *Nature*, uma revista conhecidíssima por todos nós, séria e respeitada, de um pesquisador chamado Morris, ele percebeu que, ao pesquisar os hábitos sexuais de homens e mulheres, em termos de parceiros e parceiras do outro sexo, os homens normalmente relatam um número de parceiras mulheres bem superior ao que as mulheres relatam de parceiros homens. Vocês entenderam? Ficou confuso?

Vamos lá, é como se os homens tivessem parceiras em número superior ao que existe de mulheres. Trocando em miúdos, em uma população em que há dez pessoas, cinco homens e cinco mulheres, os cinco homens relatam que tiveram



apenas uma parceira; das cinco mulheres, quatro relatam que não tiveram nenhum parceiro, e uma relata que teve um parceiro. Como é que pode isso? Ela não pode ter tido apenas um parceiro e nem todos os cinco homens tiveram uma parceira, senão, essa mulher teria que ter, no mínimo, cinco parceiros.

A discrepância na resposta, no exagero masculino, para subestimação feminina, o que é comum no relato, como identificado por nós, é um exemplo claro desse tipo de problema de pesquisa que também acaba afetando as pesquisas de cibercrime. Certo?

E esse problema aí, no caso da pesquisa do Morris, acontece muito mais, porque os homens exageram. As mulheres tendem a diminuir um pouco. Não são todos os homens que exageram, não. Incrivelmente, uma pequena fração dos homens que exagera muito, ou seja, aquele que gosta de passar uma imagem de macho alfa, talvez, acaba impactando todo o resultado de maneira geral, uma estimativa irreal. Ou seja, inicialmente, nós já temos identificados dois problemas: confiar no que os homens dizem — mulheres, será que vale a pena confiar no que os homens dizem? — e esses que nem sempre são honestos, por vários motivos, porque até possuem conflito de interesses, exageram demais.

Um problema é a concentração. Senhores, a forma mais comum de se estimar quantidades desconhecidas em uma população volumosa é através das chamadas *surveys*, pesquisas e entrevistas, pesquisas em que o entrevistador vai fazendo um questionário com cada indivíduo, para obter essa resposta em uma amostra que seja representativa de uma determinada população.

Quando isso é uma característica homogênea, distribuída homogeneamente pelo universo, é algo fácil. Basta termos pessoas suficientes, basta termos uma amostra representativa, que nós teremos aí um resultado significativo que represente a realidade.

Por exemplo, homens e mulheres, você quer saber, por causa de um fenômeno qualquer, se determinada sociedade “x” possui mais homens que mulheres, você quer saber essa proporção. É muito fácil. Eu começo a fazer as entrevistas: você é homem, você é mulher, em uma proporção significativa, e eu tenho um resultado que vai me dar uma proporção.



Agora, quando isso é algo quantitativo, ou seja, qual é a sua renda, ou no caso aqui desse exemplo, a média salarial de Brasília. Se nós nos concentrarmos em residências apenas do Plano Piloto, qual vai ser essa média salarial de Brasília? Totalmente fora da realidade que nós queremos levantar. Não é verdade? E, se nós fizermos uma distribuição aleatória, não nos concentrarmos somente no Plano Piloto, ainda assim vai haver problema? Vai, porque existe aquele ponto fora da curva que foge da norma, que vai acabar prejudicando toda a pesquisa.

Nesse caso, situações em que na população existe uma concentração muito exacerbada, amostras que não levam em conta essa concentração, apenas são amostras aleatórias, sem compensar por essa concentração, não representam uma realidade ampla dos indivíduos, representam, na maioria das vezes, uma visão distorcida da realidade.

E isso, para que eu tenha uma certa estratégia para atenuar esse efeito, tenho que me preocupar onde entrevistar, quantas pessoas de cada local, qual o peso de cada resposta. São nuances que, muitas vezes, dependem de outro trabalho científico para serem levantadas, para que eu possa ter com precisão uma representação amostral de um determinado assunto que estou tentando pesquisar.

E aí eu culmino com uma frasezinha: *“Amostras aparentemente representativas podem resultar em estimativas não representativas”*. E, para o cibercrime, isso acontece.

Olha só, em pesquisa do Gartner sobre *phishing*, encontrou-se que a perda média por incidente é de 857 dólares, contudo, a mediana da mesma pesquisa era de 200 dólares.

Vamos recuperar aqui o estudo do ginásio do que é média e do que é mediana. A média é o valor médio, ou seja, a soma dividida pelo total; e a mediana é aquele valor que, se você ordenar numericamente todos os valores obtidos, aquele ponto central, aquele que está no meio, vamos dizer que seja ordem alfabética, a pessoa que está com o nome no meio da lista, no caso de números, o número que está no meio da lista é a mediana. Se tiver número par, você soma os dois do meio e divide por dois. O número do meio era 200 dólares, mas a média era 857 dólares.

Vejam vocês, grande parte da amostra representava uma enorme concentração em uma proporção que, no caso aí, diz que 59% das perdas estavam



concentradas em apenas 1% dos entrevistados. E era esse 1% dos entrevistados que pautava a realidade de todos os demais.

A pesquisa não levava em consideração isso. O objetivo da pesquisa é o quê? É entender não o que uma ou duas pessoas têm de perda, mas entender o que a sociedade tem como um todo de perda. No entanto, a pesquisa não levava isso em consideração, porque é mais fácil fazer pesquisa assim. Você vai entrevistando pessoas até considerar que chegou a um número razoável e para. Está aí a referência. Certo?

Por exemplo, aquela pesquisa sobre a qual nós falamos agora há pouco também tem o mesmo problema. A média foi de 1.876 dólares e a mediana, 500 dólares. Olha o nível de concentração aí! Isso já excluindo aqueles dois números exagerados que falamos antecipadamente. E isso não só aconteceu para valor financeiro, não; aconteceu para horas de dar um *time*, que é o que chamamos de horas perdidas de operação.

Na verdade, isso é praxe em relatos. Essa concentração, que é um problema que desvirtua os resultados desse tipo de pesquisa, que gera números que não são representativos da realidade, é comum quando se vai relatar crimes cibernéticos.

Não sei se vocês conhecem, mas o IC3 — Internet Crime Complaint Center, que é gerido pelo próprio FBI, entre outros, em 2011 — essas estatísticas são atualizadas anualmente, mas tenho aqui para mostrar para vocês as de 2011 —, relatou que as perdas monetárias de crimes cibernéticos eram em média 5.580 dólares, quando a mediana era 575 dólares. Isso é uma desproporção de quase dez vezes, significa que 1% da população concentra 78% das perdas financeiras. E esse 1% quer pautar a política que todo mundo vai receber, como se todo mundo recebesse esse ônus.

Outro problema, sem falar na concentração — e esse problema é tão grave quanto —, é a própria resposta, que não tem verificação. Geralmente as metodologias, que pesquisam impactos financeiros do cibercrime, confiam em respostas que são dadas por quem é entrevistado sem nenhum critério de verificação. É como se você fosse parte de uma pesquisa dessas para *fitness*, e ele perguntasse quantas calorias você consome diariamente. Muito provavelmente, você iria responder um valor menor do que realmente consome. Quantos minutos



você corre na esteira? Você já iria aumentar o número de minutos. Quantas mentiras contamos por dia! Mentiras brancas para, talvez, alegrar alguém. Até para essas mentiras reconhecemos que são menos do que, de fato, são, etc. Todos temos conflito de interesses. Certo? E esse conflito de interesses não pode ser um risco para uma pesquisa que pauta políticas públicas.

Então, o que faço quando a fonte de informação que eu tenho disponível tem conflito de interesses? No caso, para quem eu pergunto quanto foi a perda com pirataria? Para quem? Eu poderia até pedir a resposta para um dos colegas da Mesa, mas geralmente a indústria do direito autoral é quem dá essas respostas.

A metodologia que vai ser usada é aquela que mais reforça o argumento deles. Pode ser até que eles estejam dizendo a verdade, pode ser até que o argumento deles seja válido, mas é muito mais fácil balizar um argumento com essa metodologia, porque ela sempre vai distorcer para mais.

Quem responde às pesquisas sobre crimes cibernéticos em geral? São as empresas de segurança da informação. Eu sou um profissional de segurança da informação, mas há que se reconhecer que esse pessoal possui conflito de interesses. Esse pessoal possui conflito de interesses.

São as pessoas que encomendam as pesquisas. Quando não são elas que fazem, são elas que financiam. Ou seja, eu tenho uma metodologia que, estatisticamente, não representa uma boa prática financiada por um grupo ou executada por um grupo que tem conflito de interesses. Como é que eu vou usar dados como esses para referendar política pública?

Olhe só um exemplo para vocês! Recentemente, a Symantec e a McAfee, duas grandes da segurança da informação mundialmente, relataram quanto custa o crime cibernético. Olhem só a diferença! Segundo a McAfee, é 1 trilhão; segundo a Symantec, são 250 bilhões, isso, porque ela já atualizou, pois eram 110 bilhões antes. Por que elas não entram em um acordo, não é?

O que é considerado custo do cibercrime? Sabe o que, às vezes, é considerado custo, principalmente em Direito Autoral? A multa que o indivíduo vai pagar, e talvez não tenha pago, eles colocam no cômputo para representar o impacto financeiro do cibercrime, assim como o custo com advogado para processar



o pessoal, o custo de um material audiovisual que nunca seria adquirido. Muitas vezes acontece isso.

Então, por que não sabemos se acontece sempre ou quando acontece? Porque, muitas vezes, essas pesquisas têm um problema metodológico de falta de transparência. O pouco que sabemos já é suficiente para não confiar nas pesquisas. Talvez exista aí até uma coisa intencional. Não sei. Não vou ser leviano, mas é importante que qualquer pesquisa, qualquer procedimento de levantamento de dados, que sirva para subsidiar uma decisão de política pública, tenha transparência para a sociedade ver o que está pautando a decisão de fato. Podemos cozinhar números e chegar a conclusões variadas. Como isso foi feito é tão fundamental como o resultado final.

Aí um exemplo do Brasil. Vamos citar aqui uma pesquisa relatada sobre pirataria e a entidade de classe relacionada com a pirataria de contrabando. Ela tem duas cifras, uma de 30 bilhões e a outra de 100 bilhões. Tudo bem, são anos diferentes, mas de onde foram tirados esses dois valores? Ninguém encontra. E um crescimento de mais de três vezes de 1 ano para o outro? A economia não cresceu tanto. Você até tenta entender os dados que são elencados, e não necessariamente eles estão incorretos. Eu não estou advogando isso...

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Eu gostaria só de informar a V.Sa. que o seu tempo já encerrou, mas vou lhe conceder mais alguns minutos para a conclusão.

O SR. PABLO XIMENES - Sim, senhor. Eu lhe agradeço. Falando aqui um pouquinho da pesquisa, que é muito divulgada, da Ipsos/Oxford Economics. Essa pesquisa é uma das mais usadas na imprensa para a pirataria de audiovisual no Brasil. Cada vez que ela está sendo divulgada, é divulgada com um valor diferente. Já foi divulgada no *O Estadão* com 4 bilhões em perdas. Em um artigo da International Intellectual Property Alliance já fala que são 7,3 bilhões em perdas. São imprecisões que precisam ser identificadas.

E o pior, essa pesquisa, em particular, vem de um artigo, o *Economic Consequences of Movie Piracy: Brazil*, de janeiro de 2011. A metodologia, senhores, que ela usa é a seguinte: entrevistas por telefone. Ela usou essa mesma metodologia para uma pesquisa equivalente no Canadá. A metodologia específica



desse estudo não está acessível publicamente, mas, como foi feita na mesma época, imagina-se que haja similaridades. Ela foi feita pela mesma organização e com o mesmo objetivo.

O que ela faz? Ela liga para várias pessoas — no Canadá ligou para 3.500 pessoas, aproximadamente, para representar todo o universo do Canadá —, faz perguntas, pega o total de pessoas que consegue estimar por aquela pesquisa como piratas e multiplica pelo total da população. Na pesquisa deu 30%, há tantos milhões de pessoas, então, 30% de tantos milhões dá tantos milhões de piratas. E aí faz mais uma multiplicação para tentar entender o impacto disso tudo.

E ainda mais, na própria pesquisa, ela admitia que eles eufemizavam a questão da ilegalidade, quase como se estivessem dando uma imprecisão aos termos “pirataria” e “ilegalidade”, para que a pessoa, em tese, se sentisse mais à vontade, o que gera um significado impreciso. Às vezes, a pessoa pode ter respondido querendo dizer uma coisa e acabou dizendo outra.

Esse é um dos grandes estudos, um dos mais referenciados, em que há um fator de impacto maior, talvez, nessa parte de impacto econômico do crime cibernético. E a conclusão desse estudo, feito por pesquisadores ligados à Microsoft — a Microsoft é interessada, então, ela tem um *buyers* para menos —, é preocupante. Eu vou traduzir só a parte em negrito, em que ela fala sobre a qualidade dessas pesquisas de cibercrime: *“Elas são tão malfeitas e tendenciosas que não se pode colocar a menor fé em seus achados”*.

E eles ainda continuam dizendo que não são os únicos que pensam assim e citam referências de outros pesquisadores de peso que concluem a mesma coisa. A referência está aí.

Eu ia falar mais um pouco, mas não tenho mais tempo, acho que essa questão ainda pode ser discutida pelos demais colegas. Eu queria fazer um apelo aos Srs. Deputados para que não confiem cegamente em pesquisas, exijam a metodologia, por mais que ela tenha sido publicada por uma instituição de renome, porque, dentro de uma instituição, existem vários grupos de pesquisa. E mesmo uma pesquisa sendo séria, feita com rigor, ela segue uma metodologia, e a metodologia pode estar equivocada. Não só o resultado final é importante, mas entender a metodologia, criticar a metodologia, chamar especialistas, contar com as



universidades brasileiras, porque elas também podem ser tendenciosas, mas pelo menos são menos tendenciosas, eu imagino. Se for entender para um grupo econômico, pelo menos é um grupo econômico nacional.

Eu concluo dizendo que as pesquisas que não consideram a desigualdade natural na distribuição, onde há concentração, ou então que não consideram a capacidade de se verificar as respostas, elas não podem ser usadas ou não deveriam ser usadas para pautar decisões. Elas distorcem a realidade.

Agradeço ao Presidente da Comissão e ao Sub-Relator da Comissão e a V.Exas. pela paciência.

Era isso que eu tinha a dizer, aliás, quase tudo que eu tinha para dizer.

Obrigado.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Agradeço ao Sr. Pablo Ximenes pela apresentação.

Nós queremos a autorização de todos os palestrantes para disponibilizar tanto para a CPI, como também colocar à disposição, as apresentações de vocês.

Convido para fazer uso da palavra o Sr. Pedro Mizukami, professor do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas.

Sr. Pedro, V.Sa. também dispõe de 20 minutos para fazer uso da palavra.

O SR. PEDRO MIZUKAMI - Muito obrigado. Muito boa tarde!

Eu queria começar agradecendo muitíssimo, em nome do Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas, no Rio de Janeiro, pela possibilidade de contribuir com os trabalhos desta importantíssima Comissão. É sempre um privilégio estar aqui. Todas as vezes que venho a Brasília, eu aprendo muitíssimo sobre Direito, sobre como as leis são feitas, sobre o Brasil e também sobre mim mesmo. Eu espero poder contribuir para que esta CPI tenha um trabalho ainda mais formidável do que já tem desempenhado.

Na verdade, aqui eu sou um verdadeiro peixe fora d'água, apesar de ser Pedro, como os demais. Não sou Pablo, mas eu sou o único representante aqui da área de Humanas, em sentido amplíssimo. Eu não tenho *background* técnico. Sou da área de Ciências Sociais Aplicadas, formado em Direito. Sou advogado e trabalho no CTS — Centro de Tecnologia e Sociedade da FGV desde 2007.



Peço permissão aos colegas para sair um pouquinho do tema mais técnico. Aliás, eu tenho certeza de que esse tema está muito bem coberto e de que a apresentação do Pablo foi uma excelente *preview* das coisas que ainda vamos abordar hoje. Vamos tentar abordar alguns tópicos mais jurídicos com vocês.

(Segue-se exibição de imagens.)

Vocês notaram que o meu título aqui é *Contribuições à CPICIBER*, não diz muito a que veio. Vamos tentar corrigir isso daqui a pouquinho.

Crimes cibernéticos. Quando falamos em crimes cibernéticos, nós nos referimos, necessariamente, à Internet. Quando falamos em Internet, falamos em regulação da Internet. Esse é um tema que está sempre no noticiário. Abrimos os jornais, abrimos os *sites* dos principais veículos e sempre vai haver alguma notícia sobre a regulação da Internet ou vai haver algum caso interessante envolvendo Internet.

Para começar, achei importante trazer aqui matéria que saiu no *The New York Times*, no dia 10 de outubro, sobre a administração americana desistindo de conseguir *backdoors* em *softwares* e aparelhos produzidos pelas empresas do Vale do Silício para efeito de facilitar acesso a dados para fins de investigações pelos órgãos de *law enforcement* dos Estados Unidos, *law enforcement* e inteligência.

Então, tanto o FBI quanto a CIA se veem afetados por essa decisão de, pelo menos publicamente, pelo menos no discurso público, anunciar que desistiram de infiltrar *backdoors* e atalhos para acesso a esses dados nesses aplicativos, nesses aparelhos. Por quê? Porque eles correm o risco de abrir o sério precedente de que esses dados e *backdoors* sejam aproveitados por Estados rivais ou até mesmo por terroristas e cibercriminosos. Esse é um dado interessante do dia 10 de outubro.

No dia 6 de outubro, o Tribunal de Justiça da União Europeia decidiu invalidar o acordo de compartilhamento de dados que havia entre Europa e Estados Unidos, chamado Safe Harbor, por meio do qual os Estados Unidos daria aos dados pessoais uma proteção similar àquela conferida pelas legislações da União Europeia. O acordo foi invalidado justamente em razão das denúncias e dos problemas que surgiram após as revelações de Edward Snowden.



Trata-se de outra notícia atualíssima que também serve como um *trailer* dos problemas e do cenário extremamente diverso e extremamente complexo dos crimes digitais e da regulação da Internet.

É um contexto internacional e transjurisdicional, que exige a compreensão e o domínio de problemas bastante técnicos, que têm múltiplas interfaces com diferentes ramos do Direito, com atividades econômicas e sociais e com discussões em andamento. É um contexto que envolve privacidade, envolve liberdade de expressão, envolve impactos à inovação, apenas para listar alguns dos potenciais pontos de contato entre o nosso tema e outras discussões, outras preocupações que observamos hoje em dia na sociedade.

Quando se fala de cibercrimes, há certa dificuldade para se atingir um meio termo, uma posição de equilíbrio entre os diversos interesses e direitos em jogo. Por um lado, existe a preocupação legitimíssima de conferir maior proteção e maior segurança à população; por outro lado, uma legislação de cibercrimes pouco equilibrada, que não dê atenção àqueles potenciais pontos de interface com outras preocupações sociais, pode desandar um pouquinho.

Então, sempre que falamos em cibercrimes, existe a preocupação de atingir o equilíbrio e um meio termo e de contemplar todos os interessados da maneira mais justa e precisa possível.

E como as senhoras e os senhores puderam perceber a partir do desenvolvimento desta CPI, uma diversidade de temas é abarcada por esse guarda-chuva amplo dos crimes cibernéticos. Apenas para listar alguns exemplos, podemos falar de crimes digitais em espécie e dos bens jurídicos que são atingidos por esses crimes digitais, podemos falar de honra, patrimônio, liberdade sexual, dentre outros. Para cada um desses interesses e bens jurídicos, talvez haja soluções diferentes.

Podemos falar de proteção a dados pessoais, de criptografia e seus usos. A criptografia tem diversos usos. Todo mundo faz uso da criptografia, às vezes, até sem saber. Toda a vez que fazemos o *login* no sistema de *home banking*, estamos usando criptografia; toda vez que navegamos num *site* de *e-commerce*, que dá proteção aos nossos dados pessoais, estamos falando de criptografia. Sem criptografia, o *e-commerce* quebra, o *home banking* quebra.



Podemos falar de anonimato e de navegação anônima. E aqui, evidentemente, há aquela célebre controvérsia da vedação ao anonimato de que trata a Constituição. Poderíamos ficar falando por horas e horas e nem chegar a um consenso de como interpretar esse artigo.

Podemos falar de navegação anônima, que é diferente de anonimato puro e simples. A apresentação que o Thiago Tavares, da SaferNet, fez aqui há alguns dias, é muito lúcida e clara no sentido de explicitar que a denúncia anônima é parte integral do sistema de proteção às crianças e aos adolescentes e a outros crimes praticados na Internet. É um tema muito complexo, um tema quente.

Podemos falar de retenção de dados, bloqueio de *sites*, neutralidade de rede e cooperação internacional. Esta não é uma lista exaustiva não, é uma lista de alguns temas desse riquíssimo cenário dos crimes cibernéticos.

Também podemos falar de processos em andamento. Além desta CPI, há o debate sobre a regulamentação do Marco Civil da Internet, que é um decreto presidencial, o debate público sobre o anteprojeto de lei para proteção de dados pessoais, a continuidade do processo de modernização da Lei de Direitos Autorais e uma série de projetos. Esta também é uma lista não exaustiva. Infelizmente a fonte está muito pequena e acho que vai dar para ler. Mas vocês sabem disto melhor do que eu: há uma série de projetos que têm sobreposições e interfaces com os temas ligados a esta Comissão.

Então, diante deste cenário multifacetado e complexo, como eu estruturei a minha apresentação para V.Exas. aqui hoje? Eu decidi me focar em dois temas, falando um pouco de retenção de dados e um pouquinho de bloqueio de *sites* em relação a violações de direitos autorais.

Vou começar por retenção de dados. Só explicando um pouquinho do contexto, para não me delongar muito nisso, que já é um tema de conhecimento das senhoras e dos senhores, o Marco Civil da Internet, ao disciplinar a retenção de dados ou a guarda de registros, de conexão e de acesso e aplicações de internet, fixou o prazo de 1 ano para registros de conexão e de 6 meses para registros de acesso. O acesso a esses dados ou a esses registros de conexão apenas podem ocorrer mediante ordem judicial.



Ele também disciplina a guarda cautelar por períodos maiores: a autoridade policial solicita; efetua-se uma guarda cautelar por um tempo superior; e existe um prazo para que o pedido judicial de compartilhamento desses dados seja realizado. Ele ainda disciplina, no art. 10, § 3º, os dados cadastrais, que são um tema bastante sensível e complicado.

Em relação à retenção de dados, acho que, como uma ilustração muito importante desse paralelismo de processos e de fóruns diferente até mesmo nesta Casa, onde essa discussão acontece, nós podemos lembrar os debates que acabaram de acontecer na CCJC a respeito do PL 215, que estabelece e estabelecia, numa versão anterior, o acesso a esses registros sem ordem judicial. Como isso acabou sendo polêmico demais, a medida caiu. E na sua versão atual, ele amplia em grau considerável as obrigações de coleta de dados cadastrais.

Em dados cadastrais, nós incluímos endereço completo, telefone, CPF, conta de *e-mail*. Isso acaba impondo o que efetivamente é na prática quase que um registro obrigatório para o uso de internet no Brasil.

As consequências disso nós estamos ainda discutindo. Mas é um ponto bastante sensível, que ilustra uma ampliação ou um desejo de que se alterem as disposições do Marco Civil da Internet em relação à guarda de dados, o que pode gerar uma série de consequências e uma série de problemas que precisam ser avaliados com bastante cuidado e cautela.

Só para trazer um pouco da discussão internacional, no ano passado saiu uma decisão do Tribunal de Justiça da União Europeia que acabou por invalidar toda a sistemática que a União Europeia tinha adotado para a retenção de dados, para a qual eles tinham um prazo fixado de 6 meses no mínimo e 2 anos no máximo. E o Tribunal de Justiça da União Europeia acabou chegando à conclusão de que em relação a direitos fundamentais dispostos na Carta dos Direitos Fundamentais da União Europeia, essa diretivas e as legislações que as implementavam deixavam muito a desejar principalmente em relação ao respeito pelo vida privada familiar e à proteção a dados pessoais. Entendeu-se que essa decisão seria desproporcional.

Eu apenas estou pincelando alguns trechos importantes. O PowerPoint ficará disponível, é claro, para consulta de todos os interessados.



Quais os pontos principais dessa decisão? A retenção de dados prevista na diretiva abrange de maneira geral todas as pessoas, todos os meios de comunicação eletrônica e todos os dados relativos ao tráfego, não sendo efetuada nenhuma diferenciação, ou limitação, ou exceção em função do objetivo de luta contra as infrações graves. Ela também não estabelece critérios objetivos que permitam delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior, para prevenir, detectar ou agir penalmente contra infrações suscetíveis de ser consideradas suficientemente graves à luz da amplitude e da gravidade da ingerência nos direitos fundamentais que a medida estabelece.

Finalmente, a decisão impõe que os dados sejam conservados por períodos não inferiores a 6 meses, não procedendo a uma distinção entre as categorias de dados em função de sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa.

Não especifica ainda que a determinação do período de conservação deve se basear em critérios objetivos, a fim de garantir que se limite ao estritamente necessário.

Então, podemos observar que há vários fatores que devem ser levados em consideração para que uma medida como a de guarda de registros atenda a requisitos de proporcionalidade. Foi isso que o Tribunal de Justiça da União Europeia decidiu.

E os países membros da União Europeia estão correndo atrás, para ver como se adequar a essa decisão. A Alemanha está com uma lei em discussão que estabelece prazos muito inferiores aos que a diretiva havia estabelecido. Essa é uma discussão que está em andamento ainda.

Na falta de critério ou de soluções, podemos ter alguns norteadores, alguns princípios norteadores que podem, pelo menos, servir de ponto de partida para discussões, ainda que esse não seja um ponto de chegada necessariamente. Então, gostaria de trazer aqui ao conhecimento da Casa esta carta de princípios internacionais sobre aplicação dos direitos humanos na vigilância das comunicações, que foi feita no âmbito do projeto *Necessary and Proportionate* (Necessário e Proporcional), duas palavras que vamos ouvir muito ainda fora do



Brasil e dentro do Brasil, em relação à privacidade e a medidas que envolvam a Internet.

Eu, como estou com tempo já um pouquinho apertado, não vou correr e explicitar cada um desses princípios, mas temos uma série de sete princípios aqui, que acho que seria muito interessante analisarmos para ver se conseguimos chegar a uma legislação que, de fato, consiga atender a esses *standards*, a esses critérios que foram, nesse caso, estabelecidos por mais de 400 organizações não governamentais que têm atuação destacada no âmbito dos direitos digitais e no âmbito da proteção à privacidade na Internet.

Vou concluir, agora falando de bloqueio de *sites*, que é um tema que está na ordem do dia, na moda, tem saído na imprensa frequentemente e também passou por uma das sessões desta Casa. Da mesma maneira, um pouquinho de contexto. O Marco Civil da Internet, no art. 9º, no que dispõe sobre neutralidade de rede, ele dispõe que: *“Na provisão de conexão à Internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo”*. Então, é vedado bloquear. A discussão que tem sido feita, inicialmente no âmbito das consultas públicas referentes à regulamentação do marco civil, ao decreto presidencial, é no sentido de tentar cavar uma exceção ao princípio da neutralidade de rede por via do decreto presidencial, o que, na minha opinião, é totalmente inviável. Para isso aqui poder ocorrer, seria necessária uma mudança legislativa, em razão do que o art. 9º, § 3º, dispõe. Se essa mudança legislativa é conveniente ou inconveniente, vamos abordar um pouquinho daqui para frente.

A proposta da Motion Picture Association, em síntese, era essa exceção ao princípio da neutralidade de rede e para a imposição do bloqueio técnico de *sites* que contenham conteúdo em violação de direitos autorais. Quais são os problemas aqui? De novo, necessidade e proporcionalidade. Esses dois critérios remetem a outros três níveis de análise que devem ser empreendidos para que tenhamos uma ideia um pouco mais clara a respeito da propriedade dessa medida. Em primeiro lugar, temos que analisar os danos colaterais a outros direitos. Não estamos só falando de direitos autorais aqui no caso. Essa medida tem potenciais impactos a outros direitos. Também estamos falando de questões de ordem técnica, problemas



de ordem técnica, que afetam a própria infraestrutura da Internet ou a maneira como a Internet funciona. Então, é importante que levemos em consideração esses problemas e, por último, a efetividade da medida, se a medida serve ou não serve para a consecução dos fins aos quais ela se propõe.

Vamos lá, um por um, rapidinho, relâmpago, nos 3 minutos que me faltam.

Um ponto de referência importante para essa discussão é o relatório do relator especial para proteção do direito à liberdade de opinião e expressão no âmbito da ONU, Frank La Rue, que, em 2011, elaborou esse relatório, que tem insumos bastante relevantes, bastante importantes para a discussão a respeito de liberdade de expressão na Internet. E ele aborda, com alguma delonga, o tema do bloqueio de *sites* e levanta preocupações com o uso de tecnologia de bloqueio e filtragem pelos Estados, por potenciais danos à liberdade de expressão. Entende que as condições que levam ao bloqueio geralmente não se encontram previstas em lei ou, quando estão, são vagas e amplas, a ponto de ensejar o bloqueio arbitrário e excessivo. Viola o art. 19, 3, do pacto internacional sobre direitos civis e políticos, e, ainda, quando justificadas, as medidas são desnecessárias e desproporcionais em relação aos fins almejados. Isso aqui é uma síntese das conclusões do relatório. O relatório integral é muito interessante e vale a pena ser lido.

A comunidade técnica igualmente vê essas medidas com maus olhos. A ICANN, no meio do seu Security and Stability Advisory Committee, esse Comitê Consultor para Segurança e Estabilidade, tem dois documentos bastante importantes a respeito de problemas potenciais no nível técnico que medidas de bloqueio poderiam provocar. Os documentos estão referenciados aqui nos eslaides.

Citando os documentos, podemos mencionar que todas as abordagens técnicas para bloqueio de DNS e, ainda mais, tentativas de contornar o bloqueio terão impacto na segurança e/ou estabilidade de usuários e aplicações. O bloqueio de acesso a conteúdo via DNS tem sérias implicações técnicas, inclusive relacionadas à segurança e estabilidade da Internet. O SSAC recomenda a qualquer governo compreender a fundo os potenciais problemas desse tipo de medida antes de partir para a implementação.

Continuando na comunidade técnica, a Internet Society, que abriga órgãos de padronização muito importantes para o funcionamento da Internet, nesse documento



Internet Society Perspectives on Domain Name System Filtering, diz que a Internet Society acredita que políticas e regulações que requerem a interrupção da infraestrutura de DNS, seja por filtragem de resultados ou por apreensão de nomes de domínio, têm sérias deficiências. Elas são facilmente contornáveis, não resolvem o problema, são incompatíveis com o DNSSEC, que é uma tecnologia para segurança de nome de domínio, causam danos colaterais, colocam usuários em risco, encorajam a fragmentação da Internet, incentivam o uso de serviços *underground*, e há preocupações também quanto a direitos humanos e devido processo legal.

Aqui, retomando o que o Pablo muito eloquentemente explicou a respeito de problemas referentes a pesquisas, a MPAA tem circulado uma pesquisa do Rahul Telang, professor do IDEA, que é um centro de pesquisas que fica hospedado na Universidade de Carnegie Mellon, a respeito dos efeitos do bloqueio de *sites* no Reino Unido, um país que implementou essa medida. Ao mesmo tempo em que temos essa pesquisa, também temos outras pesquisas que mencionam exatamente o contrário. Temos uma pesquisa da Universidade de Amsterdam, feita em parceria com a Universidade de Cherbourg, que conclui que o bloqueio feito na Holanda não teve qualquer efeito. Também temos uma pesquisa feita por um pesquisador da Universidade de Padova, no contexto da regulação italiana a respeito do bloqueio de *sites*, que conclui que, muito pelo contrário, em vez de diminuir a frequência e o uso desses *sites*, na verdade, houve um aumento devido ao efeito Streisand, que é o efeito e empresta o nome da cantora Barbra Streisand, que, quanto mais se tenta remover coisas da Internet, mais as pessoas ficam sabendo e mais elas vão atrás de procurar tal informação. Então, a conclusão desse estudo é que o efeito Streisand, a partir dos bloqueios de *site*, acabaram, na verdade, provocando picos de acesso a esses *sites* depois.

Retornando aqui ao ponto que o Pablo mencionou a respeito da confiabilidade das pesquisas, nós, no Centro de Tecnologia e Sociedade, participamos de um estudo que foi concluído em 2011, coordenado pelo Social Science Research Council, de Nova Iorque, com vários países, Brasil, África do Sul, Índia, sobre como o combate à pirataria se estruturou, como o combate à pirataria se institucionalizou nesses diversos países. Em um dos pontos principais do estudo, que eu trouxe para



distribuir aqui, temos uma versão nacional do capítulo brasileiro, que foi publicada nesse livro *Brasil Pirata, Brasil Original*, analisamos em profundidade problemas relacionados a pesquisas que tentam mensurar impactos e danos provocados por pirataria. Inclusive quanto a um dos números que o Pablo mencionou, chegamos a três números mágicos da pirataria no Brasil. Os números mágicos são: a pirataria provocaria perdas de 522 bilhões de dólares — 522, na verdade, é uma faixa que varia entre 516 e 560 bilhões de dólares anualmente, sem especificar o período anual, é claro, todo ano é a mesma coisa, muito mais do que os 360 bilhões do narcotráfico —; também causaria a perda em 30 bilhões em tributos para o Governo; e, por fim, provocaria perdas de 2 milhões de postos de empregos formais.

Tentamos pesquisar e procurar a fonte dessas pesquisas. Foi um trabalho de detetive que restou frustrado. As atribuições que eram feitas a essas pesquisas, a de 2 milhões, por exemplo, de empregos formais, era sempre atribuída à UNICAMP. Agora, quem da UNICAMP nós nunca soubemos. Houve, em certo ponto da pesquisa, que seria uma pesquisa do Pochmann. Entrevistamos o Pochmann, e ele disse: “*Não. Eu fiz uma pesquisa sobre comércio, que não tinha necessariamente a ver com pirataria*”. Enfim, era restrita à cidade de Campinas e não dava para fazer essa extrapolação. E quanto aos 30 bilhões que, às vezes, é atribuído ao UNAFISCO, não conseguimos encontrar a pesquisa por trás. Nesse sentido, é de louvar a iniciativa da MPAA de pagar cerca de 1 milhão de dólares para esse centro de pesquisa de Carnegie Mellon efetuar pesquisas de cunho acadêmico. Mas é sempre importante, em primeiro lugar, olharmos para todo o cenário, todo o contexto e todas as pesquisas que são produzidas, e, finalmente, levar em consideração os vieses que nitidamente podemos encontrar nessas pesquisas, principalmente quando se tem um órgão da indústria investindo 1 milhão de dólares em um centro de pesquisa.

Era basicamente isso o que eu tinha para falar. As conclusões são que é preciso se avaliar meios mais hábeis para lidar com a questão da pirataria na Internet; a filtragem e o bloqueio de conteúdos devem ser sopesados com esses outros meios, em uma análise de necessidade e proporcionalidade; os dados colaterais devem ser levados em consideração, tanto em relação à violação de outros direitos — liberdade de expressão, livre iniciativa, é muito importante



mencionar — quanto em relação a potenciais problemas técnicos; e é preciso contextualizar a discussão sobre filtragem e bloqueio no âmbito maior dos direitos autorais, especialmente em relação a regimes em discussão como o de *notice and takedown*, nos Estados Unidos, e, preferencialmente, um sistema superior, o do Canadá, de *notice and notice*.

Era basicamente isso o que eu tinha para expor.

Agradeço a paciência e a extensão do prazo. (*Palmas.*)

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Eu é que agradeço ao Sr. Pedro Mizukami pela palestra proferida.

Vamos passar a palavra ao Pedro Markun, que também terá 20 minutos para fazer uso da palavra.

O SR. PEDRO MARKUN - Primeiro, sei que não é muito protocolar, não sei nem se posso, mas os Deputados poderiam só levantar a mão para eu saber quem são, para eu olhar para vocês quando eu falar? (*Pausa.*)

Na verdade, é o seguinte: quando eu estava preparando esta apresentação, sugeriram-me fazer uns eslaides para entregar a vocês, porque falaram que não iria vir muita gente e quem viesse iria ficar no celular e não iria prestar atenção no que eu iria falar. Falei: "*Não! Não é possível!*"

Então, eu queria pedir um pouco de atenção, já que eu não trouxe eslaides.

Bom, meu nome é Pedro Markun.

O SR. DEPUTADO ODORICO MONTEIRO - Pedro, independentemente de estarem aqui, os Deputados depois vão ter acesso a todo esse material. Está tudo gravado, taquigrafado. Como a Casa tem uma dinâmica própria, é importante você ter a clareza de que, embora alguns Deputados não estejam aqui, muitos que integram a CPI vão ter acesso a todo o material, porque a reunião é taquigrafada. Então, pode se sentir prestigiado também, mesmo assim.

O SR. PEDRO MARKUN - Ah, não! Eu estou superprestigiado. Como o convite foi feito para que eu viesse aqui expor a vocês, para que vocês tivessem subsídios para fazer esse trabalho, fica aí. Depois passem para os colegas. Se acharem que o que eu vou falar é uma bobagem, passem para os inimigos. Mas falem para irem lá ver o vídeo. Está tudo bem, sem problema nenhum.



Meu nome é Pedro Markun. Eu tenho 29 anos, duas filhas e sou *hacker*. Mas eu nem sei se eu fui chamado aqui por ser *hacker*. Na verdade, quando eu estava vindo, eu desisti de vir como *hacker* e resolvi vir como cidadão e internauta, porque acho que esse é um especialista que, às vezes, falta neste tipo de debate.

Eu trabalho com transparência de dados, com novas formas de fazer política, de articular gente na Internet para participar dos novos processos políticos através do meio digital, porque a Internet trouxe um monte de novidades nesse campo já faz alguns anos.

Eu, dentre outras coisas, ajudei a criar o Laboratório Hacker que há aqui na Câmara dos Deputados. Quem não o conheceu, vale ir conhecer. Vale para os Deputados e vale para todo o mundo. Inclusive, a Presidente da Comissão esteve lá, na última vez em que eu estive aqui com o Ônibus Hacker. Ela foi lá conversar conosco, a Deputada Mariana, e quando ela estava lá eu disse: *“Olha, eu estou meio preocupado com essa CPI, porque toda hora que começam a falar de crimes cibernéticos, vocês começam a colocar um monte de coisas que eu não acho que são crimes”*. Eu não sei se este é o fórum melhor para discutir isso, mas, invariavelmente, eu estou certo de que isso vai acontecer e que vocês vão puxar um monte de outras coisas para colocarem nesse mesmo balaio, juntinho, do lado de roubo a banco, e eu acho isso um pouco preocupante. Mas fico feliz, porque se eu estou aqui, pelo menos, para mim, é um claro indicativo de que, apesar de o próprio Mizukami achar que tudo é crime e botar ali... Eu acho que isso não deveria estar no chapéu dos crimes cibernéticos, mas, já que está, é massa que a gente esteja escutando pessoas, inclusive, que podem dizer que acham que não.

Então, eu fiquei meio preocupado com essa história, porque, na verdade, muito do que a gente está discutindo como crime cibernético aqui — pirataria, privacidade, publicação de conteúdo difamatório na Internet — ou já é crime, independentemente de ser cibernético, ou, mais do que isso, são mudanças culturais profundas com que a gente vai ter que lidar de outro jeito que não seja colocando no Código Penal e botando gente na cadeia. Então, é uma discussão supercomplexa.

Eu não estou aqui dizendo que nenhuma dessas pautas deve ser discutida. O que eu estou querendo dizer é que a solução fácil de tipificar, colocar no Código



Penal, mandar para a cadeia ou facilitar a vida da Polícia Federal para botar gente na cadeia talvez não seja o melhor caminho, do ponto de vista da sociedade.

E aí, quando eu estava pensando nisso, eu desisti um pouco de vir aqui como *hacker* e falei: “*Olha, eu vou como internauta, como usuário da Internet, porque a maioria dos Deputados não usa a Internet como eu uso*”.

Eu nasci dentro da Internet. Eu sou internauta, e internauta não se chama de internauta. Internauta é uma palavra criada por gente muito mais velha para descrever gente que estava na Internet tempos atrás. Hoje em dia, nem isso se fala mais. Mas, beleza, é só para pacificarmos que internauta é aquele cara que cresceu na Internet, vive na Internet, cujas práticas diárias estão conectadas com tudo isso.

O que faz um internauta ou que coisas eu faço que são importantes no contexto desta CPI? Eu baixo MP3, eu assisto a seriados que ainda não estrearam no Brasil, e esses seriados são legendados por um coletivo de pessoas chamado inSanos — esse é o nome do grupo. Eles legendam coisas de graça e colocam na Internet, claramente, violando os direitos autorais da grande empresa de mídia que faz isso. Mas isso está lá. Está na Internet a legenda feita por uma galera voluntária, um negócio que é capaz de nunca vir para o Brasil. Mas tudo bem. Se eu quiser ser mais politicamente correto, posso falar que eu estou vendo uma série do Canadá, licenciada em Creative Commons, a que eu nunca teria acesso, porque não chegaria ao mercado brasileiro.

Eu acredito na Wikipédia. Isso é uma coisa que só internauta faz. Mas eu desconfio dela e de veículos como a *Folha de S.Paulo*, da mesma maneira crítica, porque eu sei que a Internet é editável.

Eu mando *nudes*. E eu não só vi o vídeo da Cicarelli e as fotos da Carolina Dieckmann, como também vi o pornô da Xuxa, só para dizer que essa é uma questão que não tem nada a ver com a Internet. O pornô da Xuxa, que ela mandou remover lá atrás, por ordem judicial... E foi por ordem judicial, diga-se de passagem. Ela não foi lá, pediu, e saíram tirando. É exatamente o mesmo problema que a Carolina Dieckmann enfrentou recentemente. Então, de novo, os problemas já existem. A Internet dá um novo corpo para eles, mas eles já existem.

Eu compartilho *meme* de gatinho falando “*I can has cheeseburger*” e qualquer outro *meme*, inclusive *meme* de uma senhora correndo de jornalista, quando



perguntada sobre contas. Então, eu compartilho *memes* políticos e *memes* não políticos. Eu crio *memes*. Se me der vontade, eu crio *memes*. Eu assisto a *Galinha Pintadinha* no Youtube, e é muito louco, porque assistir a *Galinha Pintadinha* no Youtube significa que você vai ver um vídeo flipado. O que eles fazem? Eles espelham o vídeo para o vídeo não ser detectado pelo sistema do Youtube de detecção de conteúdo com direitos autorais. E ele tem 5% de aceleração. Então, o áudio fica um pouco mais fininho e tal, mas aí também ele burla o sistema de detecção do Youtube. Há outras mil manobras para burlar essa detecção. É isso. Eu tenho uma filha de 2 anos e outra de 4, e elas veem *Galinha Pintadinha* de vez em quando.

Muito importante isto, e este é o tipo de coisa que eu gostaria muito de ver discutido aqui: eu assino termo de uso sem ler, mano. Eu começo a jogar Candy Crush ou a acessar o Facebook ou o Gmail ou quase qualquer outra coisa, e eu clico lá em “*Eu aceito*” sem ler que diabos aquela empresa está fazendo com os meus dados pessoais, seja ela nacional, seja ela internacional ou multinacional. Esse é um problema muito sério. Isso é meio criminoso na minha leitura. Eu não deveria fazer isso.

O que mais eu faço? Eu sou obrigado a usar o Internet Explorer, que é um navegador privado, para acessar uma pá de serviços públicos, e isso também é meio criminoso. A Microsoft vem aí na próxima, e aí vocês perguntem para ela o que ela acha disso, porque isso não deveria ser assim.

E aí o que eu gostaria de fazer hoje, mas não vou conseguir fazer no tempo que eu tenho, era ensinar os Deputados a usarem a Internet de verdade, a baixarem um uTorrent de raiz, porque, só a partir dessa experiência e dessa vivência — eu estou falando com muita honestidade —, só depois que vocês vivenciarem o que é a prática de rede, vocês vão ter alguma bagagem para legislar sobre isso sem necessariamente ferir, talvez não o direito, mas as práticas correntes de milhões de brasileiros. E aí, como eu não vou conseguir fazer isso em 12 minutos, eu vou fazer um apelo para vocês passarem a todos os Deputados da Comissão: procurem os seus netos, sobrinhos, vizinhos, filhos do vizinho e, numa tarde, quando vocês voltarem para a base eleitoral, falem o seguinte: “*Me ensina a usar a Internet*”. Em uma tarde, eles vão mostrar o que há de quente no momento. Talvez você não



entenda nada do conteúdo, mas fique ligado na forma, no processo, porque esse mesmo Youtube que tem *Galinha Pintadinha* tem outros milhões de coisas incríveis. Escolha um interesse particular seu, e você vai encontrar lá vídeos muito legais.

O Mizukami colocou um monte de eslaides falando das questões legais e de algumas questões técnicas. Eu poderia fazer aqui uma outra fala, mas, do ponto de vista legal, é um grande enrosco essa história de — tanto faz — *notice and takedown*. Não é legal esse negócio de você mandar um aviso e tirar o conteúdo do ar. Bloqueio por DNS é um jeito muito ruim de tirar *sites* da Internet. Tem o W3C, que também já falaram que é ruim. Todos os que entendem do que estão falando dizem que é ruim. Então, por favor, não recomendem que isso é bom, porque não é.

Eu vou deixar esse campo mais técnico e específico para a galera que tem mais gabarito do que eu, que tem doutorado e tudo o mais, mas também fico à disposição depois. Mandem um *e-mail* e eu posso explicar ou, no mínimo, encaminhar para gente que entenda.

Além do ponto de vista pragmático, do ponto de vista legal e técnico, várias dessas ideias são ruins. Algumas são meio autoexplicativas, tipo o direito ao esquecimento, não é, gente? Por favor, não dá! Não sei se vocês já estão com essa pauta em andamento especificamente na CPI, mas há essa ideia de que a gente pode tirar conteúdo verdadeiro — não estou falando de coisas mentirosas, não —, coisas verdadeiras da Internet porque essa verdade ofende alguém. Aí eu dou um exemplo pragmático da minha vida particular: ao fazer esses *sites* de transparência, eu recebo uma pá de *e-mails* de gente que doou dinheiro para candidato, pessoa física, ou doou serviço — no *site* do TSE, aparece igualzinho: 30 reais em serviço. O cara me manda *e-mail* falando: “Quando eu procuro o meu nome no Google, aparece que eu doei 30 reais em serviço para o candidato tal. Eu quero que você tire”. Aí eu falo: “Eu não posso fazer isso, porque é um *site* de transparência sobre o processo político”. Aí vem a resposta: “Não, mas a eleição já faz muitos anos. Eu nem gosto mais daquele político”. Tudo bem, mas como eu posso remover essa informação e deixar o meu banco de dados incorreto? Você vai discutir com o TSE. Se o TSE achar que aquela informação... Aí há uma discussão premente, que tem a ver com dados pessoais. Talvez seja uma das grandes discussões que a gente tem pela frente. Mas não é tirando o meu *site* do ar que você resolve isso. Você resolve



isso criando uma boa lei de proteção de dados pessoais. Esse projeto está aí, em banho-maria, já faz algum tempo.

Então, já caminhando para o fim da minha fala, na verdade, eu queria propor um outro *frame* de raciocínio para as recomendações da CPI. Não é porque ela é uma CPI de cibercrimes que as recomendações, obviamente, têm que ser: criminalize-se tal coisa. Então, uma recomendação para esta CPI é: vamos tirar a lei de proteção de dados pessoais do banho-maria. Vamos colocar isso, de fato, em ampla discussão, com consulta pública. Já rolou, mas tem que rolar de novo, porque tem que requentar mesmo. Não é só pega, edita e publica.

Não preciso nem falar — mas é sempre bom falar — da reforma da Lei de Direitos Autorais. De novo, boa parte dessas questões relacionadas com pirataria e todos esses números fazem sentido num *frame* de direito autoral que é medieval. Para a Idade Média, talvez, esses números, sejam verdadeiros, sejam falsos, façam sentido. Para o século XXI e para as redes conectadas, não fazem sentido. A gente precisa, antes de tentar resolver o problema da pirataria derrubando *site*, reformar a Lei de Direitos Autorais, para que ela faça mais sentido para a sociedade. Essa discussão vem e volta, vem e volta. A gente sabe que há grandes interesses econômicos por trás disso, e é por isso que ela volta. Acho que é o momento de esta CPI recomendar que ela vá em frente, e que a gente, de fato, leve essa discussão para frente.

Recomendação para esta CPI: não facilite o trabalho da Polícia Federal. Estou ciente de que é uma frase meio estranha, mas é a verdade. Toda vez que você facilita o trabalho da Polícia Federal às custas da minha liberdade, eu, cidadão de bem, com dois filhos... Primeiro, eu fiz esse preâmbulo para mostrar que sou um cidadão de bem, apesar de ser *hacker*. Eu sei que eles vão pedir ao mundo que facilite o trabalho deles. E eu acho que está no direito deles pedir. Mas está no nosso direito, especialmente no de vocês, que são a Casa Legislativa, ponderar os riscos que essa facilitação em demasia pode trazer para a sociedade como um todo, no que tange à privacidade. Quando você começa a argumentar isso, logo vem um e fala: “*Não tem problema, porque eu não tenho nada para esconder*”. Só faz esse tipo de discurso de privacidade quem tem alguma coisa para esconder. Isso é uma bobagem.



Um amigo meu, pesquisador no Pará, um dia desses, puxou a referência de alguém, que eu já não lembro quem é, porque na Internet é assim, as citações vão seguindo — qualquer coisa, a gente diz que é do Paulo Coelho ou do Vinicius de Moraes —, que dizia que você dizer que privacidade só faz sentido para alguém que tem coisa para esconder é análogo a você dizer que liberdade de expressão só faz sentido para alguém que tem alguma coisa para dizer. Não é. Isso é um direito que a gente tem que preservar cada vez mais.

E, de novo, eu não estou aqui tentando simplificar e dizer que nada disso é problema. Eu entendo profundamente como essas coisas são problemáticas, mas acho que a nossa discussão tem que ir um pouco além, porque o que a gente tem que entender é que a cultura se modificou, as novas tecnologias digitais trazem um novo paradigma para isso, e a nossa legislação vai ficar em descompasso por muito tempo ainda, é verdade. Mas acho que a gente tem sempre que fazer um esforço para tentar entender isso.

Não sei se isso é possível, porque eu não li o Regimento Interno na parte da CPI. Eu li quase todo, mas de CPI eu nunca achei que ia precisar participar. Não sei se o Legislativo pode recomendar coisas ao Judiciário, mas, enquanto a gente não tiver uma formação decente para os juízes sobre o que é a Internet, mesmo que seja essa de usar a Internet com o seu filho, teremos graves problemas de compreensão do que é a Internet e gente mandando fechar a Internet: *“Fecha a Internet. Bota uma cancela”*.

Da mesma forma funciona nas escolas e nos outros espaços. Há toda uma camada de maravilhosas e lindas recomendações que a gente tem que fazer para que as pessoas possam entender mais o seu direito à privacidade, o seu direito às suas informações pessoais, justamente para que elas não sejam vilipendiadas por todas essas grandes forças do mal, sejam elas ladrões de conta bancária, sejam elas as grandes associações de mídia publicadoras de conteúdo.

Eu acho que é mais ou menos isso o que eu tenho para contar a vocês. Quero só aproveitar que a Deputada chegou para dizer que eu fiquei feliz. Contei da sua visita ao Laboratório Hacker, onde a gente discutiu um pouco essa história da Comissão, e eu falei: *“Estou preocupado, porque essa Comissão vai discutir coisas que não são coisas que eu entendo como crime cibernético”*. De fato, isso



aconteceu. Mas eu estava falando que eu achei massa que, apesar disso, convidaram pessoas que não acham que isso seja crime cibernético, como eu, para expor aqui. Não necessariamente precisamos criminalizar tudo e todos o tempo todo. E eu dei uma série de recomendações pragmáticas. Depois eu vou transcrevê-las e mandar para todos.

Estou à disposição, agora, para perguntas sobre como usar a Internet, sobre como baixar uTorrent e coisas assim. Depois, sem problema nenhum, na medida do possível, eu estou bastante a fim de participar, porque todas essas legislações que saem aqui desta Casa... Só para não esquecer, cito o Marco Civil, que foi uma grande vitória da sociedade, da Câmara, do Senado e da Presidência.

Juntos, nós passamos por um processo que, para mim, foi superdoloroso, cansativo, extenuante. Desde lá de trás, quando a gente estava — pasmem! — tentando criminalizar condutas da Internet com o PL que foi apelidado de PL Azeredo — eu não gosto muito de apelidar PL com nome de Deputado, porque a gente sabe que o processo é mais embolado do que isso —, a coisa andou, e a gente teve uma ideia genial: por quê, em vez de fazer um PL que criminaliza condutas, a gente não faz um que protege direitos? E o Marco Civil é um negócio massa, que é referência no mundo inteiro. Não deu nem tempo de ele calejar ainda, e de novo já tem projetos de lei tentando criminalizar condutas na Internet ou tentando criar buracos no Marco Civil, como, por exemplo, o 215, que tenta criar pequenos buracos no Marco Civil sem nem dar tempo de calejar. Acho que vale a gente experimentar, vivenciar um pouco a Internet, antes de sair desconstruindo um troço que a gente levou tanto tempo para construir. Ficam aí as minhas recomendações.

Eu agradeço bastante o convite, a presença e a atenção a todos.

Vou responder para todo mundo que falou que os Deputados não iriam prestar atenção que é mentira. Eles prestam atenção, basta você pedir com carinho.

Obrigado. (*Palmas.*)

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Pedro. Agradeço-lhe por ter aceitado o convite. Foi um prazer tê-lo conhecido no dia da visita ao laboratório. A gente fica muito feliz com isso, até porque esta CPI é muito dinâmica, cada um com um pensamento diferente. Acredito que vocês são



essenciais para o processo em andamento, até mesmo no final, para que nossos Relatores possam ter essa contribuição. Todas as informações que você puder mandar para a CPI serão passadas a todos os membros. Fico muito feliz com a sua presença.

Concedo a palavra ao Prof. Pedro Rezende, professor de Ciências da Computação da UnB.

O SR. PEDRO REZENDE - Boa tarde a todos.

Obrigado, Deputada, pelo convite para participar desta CPI, o que muito me honra.

É um desafio falar depois de uma Mesa tão heterogênea, embora quase homogênea no primeiro nome, não é Pablo? Procurarei fazer um ponto fora da curva nos depoimentos.

(Segue-se exibição de imagens.)

Eu gostaria de trazer à atenção dos senhores um tipo de crime que não tem sido foco das discussões que já rolaram nesta e em outras CPIs que discutem crimes cibernéticos, mas que, pela definição das duas palavras do termo, poderiam e deveriam ser consideradas também crime cibernético. E o que é mais preocupante: se assim for, serão os maiores crimes cibernéticos possíveis, porque praticados em atacado e praticamente impunes, pois são invisíveis em discussões como esta.

Então, a proteção aos direitos, de que falou Markun, e o equilíbrio, de que falou Pedro Mizukami, passam por levantar o véu em cima desse tipo de crime praticado com a intervenção das tecnologias digitais para a sua materialização e envolvem principalmente a dificuldade técnica de se levantar atribuição para estabelecer autoria e culpabilidade. Talvez esse seja um dos motivos pelos quais o tipo de crime a que eu vou me referir agora tem estado fora do radar em discussões como a desta CPI.

O objetivo desta abordagem é poder levantar e iluminar um pouco melhor os riscos que considerou o Pedro Mizukami em sua fala dos efeitos colaterais imprevistos ou indesejados de atitudes precipitadas de criminalização de afogadilho em projetos de lei, como bem citou o Markun aqui, em iniciativas como os projetos de lei que estão em discussão nesta CPI.



De que crimes estou falando? Podemos classificá-los como crimes econômicos, mas praticados essencialmente com o uso de tecnologia digital. Ao final, explicarei por que a relação deles com efeitos colaterais de criminalizações precipitadas em projetos de lei, como os que estão em discussão nesta Casa. São crimes praticados em busca do controle ilegítimo, malicioso ou ilegal de fluxos financeiros.

Vou começar traduzindo uma matéria que eu achei bastante interessante. Vou resumir bem o momento em que esses crimes se tornam cada vez mais graves e cada vez mais perigosos para o momento que estamos vivendo de um *site* que trata do assunto da sobrevivência nos tempos atuais, o Modern Survival Blog:

“Vários eventos financeiros atuais indicam importante redefinição nos rumos do nosso futuro. Os donos do poder vão fazer tudo ao seu alcance para adiar um colapso, e nisso estão sendo proativos. O mundo está sufocado em dívida intransponível, e, se nada for feito, o cenário se desdobra em hiperinflação global. O resultado desse novo rumo inclui desagregação e caos. Quando o desabastecimento e a desobediência civil dispararem e o caos social se espalhar, governos se tornarão ditatoriais na tentativa de salvarem a si mesmos. Alguns acreditam que operações especiais estão em curso para preparar um vindouro reset financeiro.”

Para encadear o assunto até onde pretendo chegar, neutralidade na rede, há aqui uma matéria da *Reuters*, divulgado pela *Reuters*, de dois analistas geopolíticos da academia militar do exército chinês.

A *Reuters* divulgou esse artigo no momento em que a China era pintada como a grande vilã do cibercrime e também como quem fomenta a guerra cibernética, a ciberguerra.

Vou passar o artigo em seguida. Eu traduzi para o português um trecho que a *Reuters* publicou em inglês, no momento em que a operação psicológica que deságua em projetos de lei como os que estão sendo discutido nesta CPI inclui a demonização dos vilões da vez.



A minha leitura é que, após 2003, o foco mudou, não é mais a China a grande vilã do cibercrime e da ciberguerra. Agora, a operação em curso é aquela desencadeada pelo episódio Snowden, que é a operação de acostumar a sociedade a um regime de vigilantismo global capaz de habilitar o surgimento de um protogoverno global, baseado no controle dos fluxos financeiros.

Toda hora eu estou errando o botão de passar a transparência. Isso vai me tomar pelo menos 1 minuto, Carlos.

Assim como a guerra nuclear era a guerra estratégica da Era Industrial, a ciberguerra é a guerra estratégica da Era da Informação, e essa se tornou uma forma de batalha massivamente destrutiva que diz respeito à vida e morte de Nações, uma forma inteiramente nova, invisível e silenciosa e que está ativa não só em conflitos e em guerras convencionais, mas também se deflagra em atividades diárias de natureza política, econômica, militar, cultural e científica. Os alvos da guerra psicológica na Internet — porque mudou o assunto, já não é mais guerra cibernética, é guerra psicológica? —, no meu entender, é porque o plano ou a esfera psicológica, a mente das pessoas é o fronte decisivo dessa guerra moderna que está sendo travada hoje, se expandiram da esfera militar para a esfera pública. Nenhuma nação ou força armada pode ficar passiva e se prepara para lutar na guerra da Internet.

Para esclarecer melhor como essa guerra está sendo travada, eu trago à luz a análise de uma grande estrategista e analista econômica que eu procuro acompanhar, ex-assessora do Ministério da Habitação do Governo Reagan nos Estados Unidos, chamada Catherine Austin Fitts. Ela tem um *site* chamado *Solari*. Essa frase eu tirei de uma palestra que ela proferiu e está no Youtube:

“O cerne da ‘guerra da internet’ é pela centralização do controle de sistemas de fluxo de pagamentos: O colapso do dólar e a imposição de outra moeda” — que pode ser o yuan, pelo volume que alcançou de fluxos — “como reserva de valor e no comércio internacional dependem desse controle: ‘quem controlar as vias digitais, os canais submarinos e satelitais’” — basicamente pontos de troca de tráfico



internacionais — “*controla a moeda global. Tarefa que tem requerido cada vez mais violência*’.”

Exemplos que podem ser de violência ao estilo de ataque de bandeira falsa para controlar movimentos, por manipulações financeiras que saem do controle, quedas na operação do pregão da Wall Street, por mais de 3 horas, no mês de julho; queda nas atividades do pregão da Bolsa de Moscou, no mês de agosto, por mais de 3 horas também, sendo que esses centros de processamento de dados, os pregões da Bolsa de Nova Iorque e de Moscou, são os centros de processamento mais resilientes que podemos imaginar do ponto de vista do projeto. São cinco níveis de *backup* para evitar que saiam do ar. Podem ter sido ataques cibernéticos de economias concorrentes, pode ter sido ataque autoinduzido para conter certo colapso de manipulação que teria saído do controle.

O que estou chamando de terrorismo econômico? Basicamente os crimes praticados por manipulação massiva de mercados com pregões eletrônicos, de maneira desleal, para usar um termo do Banco Goldman Sachs.

Aqui um exemplo de como essas coisas acontecem fora do radar de discussões políticas como essa, onde o poder econômico é visto como algo transparente.

Alguém já ouviu falar desse sujeito aí, um *hacker* como Markun? Sergey Aleynikov era um programador que trabalhava para o Banco Goldman Sachs. Quando ele pediu demissão, o Goldman Sachs desconfiou que ele podia ter levado uma cópia do *software* que ele desenvolveu para Goldman Sachs, denunciou ele por roubo do código fonte que ele foi pago para desenvolver para a Goldman Sachs. Em 48 horas ele foi preso, o material de informática na casa dele foi apreendido e passou a ser vigiado mais do que o material, as barras de ouro que estão em Fort Knox, no Kansas. O Banco Goldman Sachs alega que o *software* poderia ser usado para manipular o mercado de forma desleal. Mas o que exatamente o Goldman Sachs faz com esse *software*? Ninguém viu, não é? Só viu do Markun? E por que o Governo dos Estados Unidos está protegendo esse *software*, em vez de analisá-lo para determinar como pode ser usado para manipular mercados?

Bem, o Markun disse que ensinaria como usar a Internet. Eu vou aproveitar o meu tempo para explicar um pouquinho o que é HFT, High-Frequency Trading, é



você usar a velocidade do seu processamento de dados para ganhar em cima dos trouxas que estão te usando como cliente. Toda vez que você bota uma transação de compra ou de venda de ações, se eu conseguir chegar no pregão antes de você, eu intermedeio a compra, porque vai poder fechar negócio com você por estar tendo uma diferença entre o que está sendo pedido e ofertado, eu entro no meio e corto a metade desse lucro, embolsando a metade, porque eu consigo chegar antes do meu cliente.

Então é por isso que algumas financeiras alugam, a peso de ouro, andares no mesmo prédio que opera o pregão, para terem a diferença de alguns milissegundos ou nanossegundos, para chegarem aos seus pacotes antes que os concorrentes.

Isso pode ser considerada uma atividade ilegal? Do ponto de vista do Direito Econômico, se não está regulamentado como prática desleal econômica, sim, mas, do ponto de vista da capacidade técnica de operar tal tipo de *software*, trata-se de uma questão de neutralidade em relação ao que pode e o que não pode ser praticado como privilégio.

Exemplo de uma empresa que opera com HFT, a primeira, a pioneira, a Victor Finance, só teve um dia com perdas em 6 anos de operação na Bolsa de Valores. Durante o primeiro julgamento, em que o réu foi condenando, cumprindo pena, enquanto aguarda o segundo, os promotores americanos pediram sessão secreta ao juiz quando detalhes sensíveis do *software* de HFT fossem discutidos.

O que esse *software* pode fazer? Mesmo bloqueando a discussão técnica de como o *software* funciona, os efeitos aparecem.

Banqueiros finalmente admitem para o investigador britânico manipulação no mercado de juros, na Inglaterra, LIBOR.

Fraudes que produzem efeitos desleais em mercados de câmbio foram admitidas. O problema é que a punição, quando ocorre, só em multas, e bem menores que o lucro com as fraudes. Nenhum técnico que desenvolve *software*, nenhum diretor que encomenda *software* para essas casas bancárias se sente desestimulado por essas condenações por prática desleal de atividade financeira, porque a multa, quando é aplicada como pena, recai sobre os acionistas do banco e não sobre... A condenação não é criminal, é civil.



Bem, se você quer ter uma ideia de como a multa também termina sendo um estímulo para a prática cada vez mais frequente e continuada desse tipo de crime, basta observar a proporção. As multas aplicadas a Goldman Sachs, Bank of America, Citibank, Barclays, BNP Paribas, HSBC, J.P.Morgan, RBS e UBS — RBS, escocês; e UBS, suíço dão um total de 2 bilhões de dólares, por praticarem manipulação de mercados de câmbio e de juros, durante 5 anos, num mercado em que circulam 5.3 trilhões de dólares por dia. As multas a esses bancos representam um dois mil avos do giro diário.

E o Brasil? Como é que fica? A moeda brasileira está sendo objeto de manipulação indevida nesses pregões, conforme denúncia do *Bloomberg News*, junto com o rublo, moeda da Rússia. Não deve ser à toa que a Rússia está pagando 14% de juros nos títulos da dívida pública, e o Brasil também, enquanto os bancos do primeiro mundo estão pagando 0% de juro nos seus títulos, permitindo que a dívida deles cresça sem nenhuma crise fiscal como a que estamos vivendo agora por causa do juro exorbitante que se equilibra na SELIC.

A manipulação de mercados de câmbio por bancos que são compradores diretos — *primary dealers* — do Banco Central do Brasil empurra a taxa SELIC para níveis extorsivos, inexplicáveis, apenas como *spread* de risco. Praticamente metade do círculo de 12 *primary dealers* do Banco Central do Brasil está incluída nessa lista aí. Empurram a Taxa SELIC para níveis extorsivos, inexplicáveis como apenas *spread de risco*.

Gente, a teoria econômica clássica deixou de funcionar com a Internet. Os economistas também, Markun, precisam aprender como a Internet funciona para saber como eles podem estar sendo enganados a respeito da desconexão entre suas teorias e a realidade econômica que estamos vivendo. Nenhum pregão hoje que é manipulado sorratamente ou maliciosamente por instrumentos digitais consegue formar preço conforme a teoria clássica econômica.

Bem, apesar do que vocês viram aqui, que esses bancos estão sendo processados nos Estados Unidos por estarem manipulando a moeda brasileira junto com a russa, não contem com isso para eles se sentirem desestimulados, porque a Attorney General, o Ministério Público americano, acabou reconhecendo que



exagerou na dose e que mesmo aquela punição cosmética expôs de maneira excessiva e desnecessária os bancos a uma quebra de confiança dos seus clientes.

Por isso, depois de publicada a matéria, uma nova política foi estabelecida pelo Ministério Público americano de que os grandes bancos não vão mais ser punidos por manipulação de mercado, só os funcionários de segundo escalão para baixo.

E o que acontece quando essa manipulação cria distorções como juro a 0% no centro do capitalismo e juro a 14%, 15% na periferia do capitalismo, considerando a Rússia parte da periferia? Quando o juro chega a ser negativo, o estímulo para o correntista é sacar dinheiro do banco e guardar no colchão, para ele não ter que pagar ao banco para guardar o dinheiro dele.

Então, qual é a maneira de você poder cobrar das pessoas para depositarem no seu banco se você está cobrando para manter o dinheiro delas no seu banco? Dificulta que elas saquem em espécie o dinheiro. E essa prática está acontecendo nos países que estão praticando juros negativos. Já são 22 no mundo hoje.

O que isso tem a ver com o assunto desta CPI? Se eu não estourar meu tempo, eu consigo chegar lá. Que estamos indo na direção, que isso tudo é preparação para outro governo global de natureza fascista fica claro quando o chefe da NSA — National Security Agency, na época do escândalo do Snowden, por motivos políticos teve que sair e fundou uma empresa de assessoria. Está vendendo agora aos grandes bancos os serviços dele para convencer o Congresso a aprovar uma nova norma que cria um conselho de guerra cibernética formado por estrategistas do Governo americano e executivos de grandes bancos. Na definição de Mussolini, isso é que é o fascismo: aliança do grande capital com o grande Estado.

No tempo em que me resta... O que isso tem a ver com o assunto desta Comissão Parlamentar de Inquérito? Se você pensar que todo esse controle financeiro na mão de poucos só era possível porque, antes da Internet, a emissão de moedas só podia ser controlada com as propriedades que caracterizam dinheiro e moeda, quando a emissão era controlada por uma entidade só, o Banco Central, com a Internet, com as moedas criptográficas, isso deixou de ser uma necessidade.



É possível a gente ter alternativa na qual o controle da emissão de moeda não precisa mais ser centralizado em uma entidade só. Isso vai ser possível, num momento de crise, em que o dólar entra em colapso, as moedas e o crédito somem e há um colapso na distribuição de recursos por conta de um colapso financeiro global no planeta? Bem, as criptomoedas estão aí para substituir, sem a necessidade de um Banco Central para colocar ordem no sistema financeiro. Mas, para isso, a Internet teria que funcionar de maneira neutra. Esse momento está se aproximando. Os sinais disso estão visíveis na combinação de dois parâmetros que estão sendo percebidos nos mercados, nos pregões eletrônicos, que são: o aumento da volatilidade combinado com a diminuição do volume. Isso é um sinal claro de manipulação excessiva, desleal.

Que a gente sofre mudanças na natureza do dinheiro, na medida em que as tecnologias evoluem, isso parece claro. Antes da revolução industrial, antes da imprensa se sofisticar ao ponto de o lastro do dinheiro não precisar mais ser no material que produz a moeda, quando as moedas que eram reserva de valor no planeta — sempre apoiadas pelo poderio militar de uma potência hegemônica — deixaram de ter lastro em metal nobre e passaram a ter lastro em papel fiat, a tentação de abusar da capacidade de controlar a emissão da moeda nunca sofreu resistência suficiente.

Todos os impérios que foram emissores de moeda que funciona como reserva de valor, impressa em papel, em algum momento sofreram hiperinflação: a França, a Grã-Bretanha e os Estados Unidos.

E o que vai acontecer daqui para frente? A Internet vai mudar a necessidade de que a moeda tenha lastro em papel? Muitos sinais de que não necessariamente precisa continuar tendo lastro em papel estão aí. Mas, sem o princípio da neutralidade na Rede, quem controla a infraestrutura de comunicação digital do planeta vai poder inviabilizar ou viabilizar alternativas aos sistemas que nós temos aí.

Por isso, Deputada, mexer com a neutralidade na Rede é uma bomba-relógio sem percepção de tamanho para quem está tentando fazer isso dentro de uma Casa legislativa, despreocupado com a visão geopolítica que eu estou tentando trazer aqui para V.Exas.



Então, minha recomendação é que não mexam na neutralidade da Rede sob qualquer pretexto. Não é perseguir ladrão de galinha que vai resolver os problemas. Vai detonar uma bomba-relógio que V.Exas. estão vendo aqui.

Muito obrigado pela atenção de V.Exas. (*Palmas.*)

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Prof. Pedro, pela sua participação, por aceitar o nosso convite e também pelas sugestões a esta Comissão.

Se o senhor puder, solicito mandar também algumas sugestões pelos *e-mails* da Comissão Parlamentar de Inquérito, para que nós possamos passá-las aos demais membros que não estão aqui hoje na Comissão.

Temos aqui alguns inscritos.

Eu fiz um bloco de perguntas e passo para todos os que tiverem a necessidade de respondê-las.

Com a palavra nosso Sub-Relator, o Deputado Rodrigo Martins.

O SR. DEPUTADO RODRIGO MARTINS - Sra. Presidente, obrigado pela palavra. Quero dizer que, como Sub-relator da área de segurança, nós escutamos primeiramente várias áreas ligadas principalmente à segurança, várias autoridades do assunto da área de segurança também. E muito se questionou sobre o Marco Civil da Internet. E aqui eu quero externar a minha alegria de ouvir a participação do Markun, em que ele vem como internauta, usuário, colocar os seus pontos de vista. Quero dizer a ele que também não tenho muito mais idade do que ele, não, tenho 33 anos, então vivenciei a entrada na Internet, não vou dizer que já nasci dentro da Internet, mas muito acompanhei.

Lógico que se faz necessária uma discussão sobre alguns aspectos abordados aqui por você — permita-me chamá-lo de você — e posso dizer também que já vi operar todos esses sistemas aí, principalmente no que diz respeito aos sistemas que baixam alguns tipos de aplicativo, ou de seriados, ou de filmes, inclusive alguns com tradução e legenda, antes mesmo do lançamento. Seria crime? Não seria? É algo de que a gente precisa. Mas eu quero fazer um questionamento a ele porque muitas vezes... Muitas vezes você repetiu que não seria necessário facilitar ou que não seria bom facilitar o trabalho da Polícia Federal. Nós sabemos que o Marco Civil dá o direito ao cidadão de ter a sua privacidade preservada, no



sentido de não ter dado ou não ter sido propiciado, pelo menos legalmente, não sei se através de um *hacker* isso pode ser quebrado ou descoberto, mas de não ter acesso ao conteúdo que o usuário acessou ou que ele viu, onde ele navegou. Mas se faz necessário, e algumas autoridades aqui, inclusive alegando risco de vida, alguns tipos de crime, externaram a vontade de que o IP da pessoa fosse disponibilizado, o IP de acesso do cidadão, fosse disponibilizado sem que houvesse a necessidade de uma ordem judicial.

E uma analogia, eles fizeram como se fosse uma RG, um CPF da pessoa. Eu quero ouvir a opinião desse usuário, do internauta a respeito do dado de acesso ao IP, para dizer que aquele IP realmente foi acessado pelo usuário, por exemplo, Rodrigo Martins, e foi acessado naquela residência ou naquele local. Eu queria ouvir a opinião sobre a possibilidade de flexibilizar esse aspecto, sendo preservada toda a privacidade de antes, tendo em vista alguns temas importantes. Você é pai de duas filhas, eu também sou pai de duas meninas, uma de sete e outra de dois, e nós sabemos dos relatos de vários tipos de crime que tem na Internet de abuso, de pornografia infantil, de sequestro, de venda de crianças. Então, eu quero ouvir o seu ponto de vista no sentido de que facilitaria nesse aspecto, somente.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Rodrigo Martins.

Concedo a palavra ao Deputado Odorico Monteiro, um dos autores dos requerimentos.

O SR. DEPUTADO ODORICO MONTEIRO - Obrigado, Sra. Presidenta, Sras. e Srs. Deputados, saúdo todos os nossos convidados. Parabenizo a Presidenta também pela forma como compôs a audiência pública. São vários requerimentos, de tempos diferentes, eu quero parabenizar, acho que foi uma audiência pública para nós muito esclarecedora do ponto de vista do que representa verdadeiramente essa questão do crime cibernético. Acho que foi uma audiência pública para nós muito esclarecedora do ponto de vista do que representa verdadeiramente essa questão do crime cibernético, e apontando questões para o futuro e eu acho que também desconstruindo alguns mitos, que muitas vezes têm aparecido aqui não só na nossa Comissão, mas como na Casa. Então, nós estamos vivendo um momento de ressignificação de valores. O século XXI é o século da informação, a superação do



modo de produção do século industrial, do século XX, para o século da informação, ou seja, a transição do modo de produção é sempre um momento em que tanto na infraestrutura da economia da sociedade, mas na superestrutura, na disputa de valores, essa coisa se dá muito fortemente. E aqui na Casa, não só na questão do crime cibernético, mas em vários outros grandes temas que nós estamos discutindo esse confronto entre os valores da sociedade são muito presentes. E eu acho que essa audiência pública foi muito esclarecedora.

Sem dúvida nenhuma, eu acho que uma coisa importante que ficou muito presente em todas as quatro falas dos quatro Pedros, três Pedros e um Paulo, é que há valorização do Marco Civil da Internet. Então, essa preocupação, e aí eu queria, o Markun acho que falou muito, usou uma expressão que me parece muito interessante: querem abrir “buracos” no Marco Civil da Internet.

Então, eu queria ouvir de vocês sobre reforçar essa questão de como nós temos que reagir e como esta CPI deve se expressar, à luz do Relator e da Presidenta, sobre os “buracos” que estão querendo abrir no Marco Civil da Internet, que me parece uma das legislações mais avançadas do mundo. Então, acho que isso é uma coisa importante, está muito forte aí na fala de vocês.

A outra questão também, e aí eu acho que o Pedro Mizukami falou muito sobre essa questão dos dados, ou seja, sobre os bancos de dados, como é que você tem a reserva. Então se entende adequado coletar dados pessoais em antecipação de todos os usuários da Internet para auxiliar posteriores investigações policiais. Porque se nós estamos discutindo também o crime cibernético, outro grande debate que tem aqui na Casa é sobre certa paranoia que se cria sobre essa questão de como a Internet pode auxiliar a investigação policial, essa coisa toda. Então, essa é uma coisa que eu queria ouvir de vocês também, que eu considero importante.

Para o Pedro Mizukami é o seguinte: o Ministério da Justiça está colocando em consulta pública um projeto de lei que trabalha a questão da proteção dos dados pessoais, e que deve ser lançado aqui dia 20 de outubro. Então, eu queria ouvir sua opinião sobre esse anteprojeto do Ministério da Justiça, sobre essa questão de proteção de dados pessoais. Acho que esse é um tema que é muito forte aqui, o debate, eu queria ouvir sua opinião.



A outra questão, um tema também muito forte também na CPI, e aqui vale para todos, é o seguinte: o quê vocês têm a dizer sobre os dados referentes à chamada pirataria de direitos autorais, que foi bem tocado pelo Pablo, foi bem tocado por vocês, mas esse é um tema que apareceu muito fortemente na última audiência pública, e eu gostaria que vocês aprofundassem um pouco essa questão da dimensão dos direitos autorais. Eu acho que já ficou claro aí que os valores que são dados ainda não são bem mensurados, mas esse eu acho que esse é um tema importante de ser discutido.

Então, basicamente, são essas três questões que eu considero importantes ouvir de todos, especificamente dirigida para o professor da FGV.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Eu é que agradeço. Obrigada, Deputado Odorico Monteiro.

Concedo a palavra ao Deputado Ronaldo Nogueira.

O SR. DEPUTADO RONALDO NOGUEIRA - Quero cumprimentar a nossa Presidenta, Deputada Mariana, que tem conduzido de uma forma muito especial esta Comissão, e eu tenho a plena certeza de que ela trará resultados significativos para o nosso País, para a sociedade, principalmente nesse contexto que é muito complicado de você compreender no que diz respeito ao conceito principalmente de crimes cibernéticos.

Cumprimento os convidados que atenderam o convite e trouxeram aqui informações que são preciosas. Na realidade, nós tivemos uma aula aqui. Depois, nós haveremos de rever os conteúdos, porque as informações trazidas enriqueceram muito esta Comissão.

Eu gostaria de fazer uma pergunta aqui, até porque eu acredito que um dos temas que mais têm trazido preocupação não somente para a sociedade, mas para os próprios órgãos de segurança dos governos, o Estado, enfim, os usuários, os provedores, as empresas, todos os atores que são de interesse, nesse mundo da Internet, é no que diz respeito à neutralidade da rede.

Tanto o Pedro quanto o professor que antes fez a sua explanação aqui nos trouxeram alguns conceitos e algumas informações que nós julgamos serem interessantes nesse aspecto.



Eu não sei quando nós vamos conseguir, na realidade, ter um conceito objetivo, definido, na forma de atuar e oferecer segurança para as pessoas sem que muitas vezes você venha transgredir direitos individuais, tanto daqueles que são, muitas vezes, impactados com alguns conteúdos quanto aqueles que se acham no direito da livre iniciativa de expressão.

Então, você colocar uma linha de proteção e de limite nesse aspecto, principalmente na Internet, é muito complicado. E tem outras variáveis também que agora nos trouxe aqui, não somente aquelas no que diz respeito à insegurança que os Estados têm, no que diz respeito aos dados ali disponibilizados e estratégias de segurança nacional, como é vulnerável nesse aspecto.

Parece-me que a Internet vai ser a ferramenta que vai encaminhar para uma unidade global, não somente no aspecto financeiro, mas de cultura também, porque ela não permite a clareza dos limites de atuação de quem ali opera, mas, principalmente, a opinião de vocês a respeito de uma legislação que não fosse um retrocesso ao conceito da neutralidade de rede, não é?, mas essa legislação também protegesse alguns valores no que diz respeito aos direitos individuais do cidadão, porque, a partir do momento, às vezes, até... Porque nem todos aqueles que operam, que têm o controle, que publicam, que se utilizam da Internet para publicar, para “esbrotar”, são pessoas que têm um comportamento ético. E, muitas vezes, quando um fato, mesmo que seja mentiroso e criminoso, ele vem a ser propagado, traz danos, muitas vezes, irreparáveis, de imagem.

Pela expertise que os senhores têm nesse aspecto, qual a sugestão que vocês dariam para o Parlamento, para esta Comissão atuar numa legislação que não trouxesse retrocesso no conceito de neutralidade de rede, porque esse é o encaminhamento que se dá no âmbito global, mas também trouxesse segurança para o cidadão.

Eu vou citar um exemplo aqui para os senhores. Casualmente, eu estava na minha cidade participando de um aniversário onde tinham algumas crianças. Eu conversei com um pai, porque ele estava muito preocupado, porque ele pegou o *tablet* de um de seus filhos e era um menino de 9 anos de idade.

O pai entrando no histórico desse *tablet* observou ali conteúdos que não seriam conteúdos adequados, tanto no aspecto de pornografia quanto também de



violência, para uma criança dessa idade, que está formatando ainda os seus conceitos no que diz respeito a valores e caráter. E o ser humano é resultado daquilo que engorda os seus pensamentos. A Internet é atrativa, ela é um mundo que não tem fim.

Aí, eu pensei: nós estamos lá com a CPI dos Crimes Cibernéticos. Talvez, através de uma legislação, seja proposto que os *sites* que trabalham com esse tipo de conteúdo tenham que ter uma chave identificando se a pessoa tem o direito de entrar naquele portal, mas ele tem que identificar ali o seu CPF, a sua idade, para comprovar que a sua idade é adequada para ter acesso àquele tipo de conteúdo.

Dizer que isso é responsabilidade da família, nós não podemos ser hipócritas e entender que o pai e a mãe vão ter condições de estabelecer uma vigília onipresente e onisciente sobre as crianças 24 horas por dia. E as crianças são curiosas.

Então, seria nessa linha a minha pergunta aos senhores: qual seria a forma que nós poderíamos, através desta Comissão, propor uma legislação que fosse moderna e trouxesse alguns contrapesos aí, para que possamos proteger principalmente aqueles que ficariam vulneráveis a essa neutralidade?

Obrigado, Sra. Presidente.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada, Deputado Ronaldo Nogueira. Agora, vamos passar às respostas.

Concedo a palavra ao Diretor Pablo Ximenes.

O SR. PABLO XIMENES - Olá. Eu vou tentar responder as perguntas mais técnicas, porque eu também sou *hacker*. Mas, agora, como estou diretor de um órgão público, a gente se apresenta como diretor. Mas já encontrei muita falha de segurança, desenvolvi muita coisa.

Vou começar com esse último questionamento. Vou falar da minha experiência pessoal. Eu tenho uma filha de 9 anos e tenho um filho de 2 anos. Sou pai de família também, um homem de bem. Como pai de família, preocupo-me exatamente com isso daí que o senhor acabou de dizer, nobre Deputado. É uma preocupação constante. Agora, a gente tem que entender uma coisa sobre a Internet. Quem quiser entender a Internet, tem que entender isto: a Internet traz uma lógica meio matemática, meio tecnológica e ela transforma a realidade. Então, não



adianta querer colocar a Internet na realidade antiga, não funciona. Ela vai encontrar contornos, vai encontrar mecanismos de superar aquela norma, aquela lei. Não se muda a Internet por decreto. Não se muda a Internet por decreto, pelo contrário, a Internet cria novas relações, novos comportamentos.

Então, com a minha filha, eu não tenho como — isto todo mundo tem que entender — criar uma chave. Tecnicamente é inviável criar um mecanismo tecnológico, baseado em uma norma, ou seja, uma vontade de manter o *status quo*, de certa forma, para que a tecnologia se adapte, a tecnologia que foi feita para ser livre, a Internet, que foi feita para ser livre, para uma dificuldade de mudança contextual. Primeiro, tecnicamente seria um pandemônio. Existe uma coisa chamada infraestrutura de chaves públicas brasileiras, que é o ICP Brasil, todo mundo usa certificado digital. Isso é supercomplicado de fazer, para situações que até exigem certa atenção, porque implica às vezes até em acesso à democracia, plebiscitos *online*, por exemplo, que ainda não estão normatizados, mas são um futuro bem presente.

Mas eu não posso simplesmente ignorar tecnicamente como a coisa funciona e tentar adaptar a Internet ao um padrão de pensamento que precisa mudar. Então, o que faço em casa, por exemplo? Eu dei um *tablet* à minha filha de 9 anos. Um *tablet* em que, inicialmente, instalei alguns aplicativos de controle parental. Eu censurava minha filha? Não, eu monitorava, fazia certa censura, mas uma censura sempre baseada no diálogo: “*Minha filha, você não pode ver tais conteúdos por enquanto, entenda, porque você não está preparada*”. Sempre que eu entendia que ela estava preparada, e posso me equivocar, eu conversava com ela.

Então, eu não blindava a minha filha de ser exposta a qualquer coisa. Eu preparei a minha filha para ser exposta a tudo. Vejo que os pais devem se adaptar à nova realidade que a Internet traz. Foi isso que eu fiz dentro de casa.

A minha filha chega, e às vezes eu estou assistindo a um filme cujo conteúdo possa lhe causar medo à noite. Ela cobre os olhos e diz: “*Posso ver, papai?*” — é até engraçado. Ela se tornou copartícipe. Isso aproximou o pai da filha — vejam que bacana! Isso construiu uma família mais unida. Agora nós conversamos. É uma cultura de convencimento, e eu tenho que convencer minha filha de 9 anos de que



conteúdos “x” são bons. E ela me convenceu. Ela tem 9 anos e já está vendo conteúdo de 12 anos, em vários canais.

Há talvez um risco muito maior e muito mais grave do que a exposição que a Internet traz: a publicidade infantil que existe no meio desses canais. Para isso eu não consegui preparar direito a minha filha. Eu tento, mas pega na jugular, e ela quer comprar isso, quer comprar aquilo, quer ter isso e quer ter aquilo. Ela sentiu uma necessidade que nunca havia sentido. Isso constrói um valor em conteúdos de até 5 anos, 6 anos.

Existe um canal para bebês que meu filho adora, a *TV do bebê*, em inglês. Ela às vezes fica hipnotizada também. Esse canal não tem publicidade infantil. Acho isso bacana.

Talvez as crianças estejam mais frágeis aí em coisas que estão misturadas. Há que se pensar nisso. Mas, de qualquer maneira, a estratégia que eu adoto é de prepará-la para ser exposta e não sonhar com uma coisa inviolável e que ela nunca vai ser exposta. Compramos, eu e minha esposa, para ela um livro que trata de sexualidade, para ela entender o que é a sexualidade, um livro escrito para a idade dela, com conceitos, para ela entender de onde vêm os bebês. Ela ganhou esse livro com 9 anos. E assim vai.

Eu entendo que isso é uma revolução que a Internet traz. Muitas vezes, tentamos não correr o risco ou fazemos um esforço ao passar por essa revolução. Eventualmente, iremos colidir com essa revolução. Não se muda a Internet por decreto. A Internet está aí. O próprio direito autoral é um exemplo disso, já partindo para a outra resposta.

É um modelo econômico em que vou remunerando; é um bem intangível que se reproduz por mágica. Antigamente, eu ainda tinha o insumo do papel, ainda tinha que criar coisas físicas. Agora, com a revolução da informação, é algo fácil. Há lucros vertiginosos que não são equiparáveis ao trabalho intelectual que gerou esse produto, essa propriedade intelectual. Vários modelos vão surgindo, mesmo com leis bem rigorosas de direito autoral, nos países dessas próprias leis, como o modelo de subscrição por conteúdo, em que se acessa o conteúdo que quiser. É admitir que agora tem que compartilhar. É admitir que não adianta ganhar pela coisa em si, e, sim, por dar uma infraestrutura tecnológica de compartilhamento, por dar serviços,



por dar um valor agregado que não somente o elemento. Há essa revolução na Internet, é preciso que se entenda; pode-se criar a lei que for.

O próprio DMCA americano está revelando, em vários estudos, que eu não apresentei aqui, pouquíssimo sucesso para se inibir a violação do direito autoral. E traz um risco colateral, complementando até o que meu colega Pedro falou — os senhores tentem adivinhar qual dos três. Ele traz efeitos colaterais severíssimos que dizem respeito à censura.

Há pessoas na Internet, até no Brasil, que formatam um determinado conteúdo que está publicado e que não é do seu interesse em uma violação de direito autoral. E mesmo não havendo legislação no Brasil para isso, como os grandes provedores de conteúdo seguem a lei americana, eles usam o chamado *notice and takedown* da lei americana, que é uma medida que deveria ter sido uma forma de criar uma exceção, para que os provedores de conteúdo não fossem responsabilizados pela violação de direitos autorais, a questão acabou se tornando um grande problema para o usuário. O que acontece? Manda-se uma carta, sem nenhuma anuência do Judiciário, e, se o provedor de conteúdo não remover o conteúdo, ele responde solidariamente com quem publica. Se ele remover o conteúdo com velocidade, ele não responde.

O problema é que 50 milhões de requisições como essas foram mandadas só para o *Google* no mês passado. Como é que um provedor brasileiro vai competir para ter infraestrutura? Ninguém lê essas requisições. É muito melhor aceitá-las, remover o conteúdo, do que criar qualquer óbice, apesar de o *Google*, parabene-se aqui, usar vários mecanismos para poder analisar com cuidado essas requisições.

Voltando à questão do endereço de IP, a esta eu quero responder, porque é um pouco mais da minha seara técnica. Eu já colaborei em várias investigações policiais que envolviam questões de crimes cibernéticos com a polícia do Ceará.

Em primeiro lugar, é preciso desmistificar isso. Até entro em conflito com o pessoal mais progressista com relação à interpretação de endereço de IP como dado pessoal. A interpretação é um pouquinho mais complexa do que isso. Mas é preciso que se desmistifique inicialmente a questão de quem tem acesso ao seu endereço de IP. Quando se vai fazer uma conexão na Internet, passa-se por saltos,



por vários saltos, que são computadores intermediários, até se chegar ao seu destino. Todos eles possuem de certa forma a informação do seu endereço de IP e, se quiserem, podem guardar esse endereço de IP, o que muitas vezes é necessário, por questões de segurança cibernética. Não tenho como fazer muitas das técnicas de segurança que protegem o usuário, técnicas históricas que vêm do começo da Internet, se eu não puder guardar o endereço do IP. Proibir-se a guarda de endereço de IP é uma coisa contraproducente em termos de segurança da informação.

Por isso, não se pode pensar numa legislação que crie óbices para essa guarda. Eu acho que isso tem que ser uma decisão, uma conversa entre o provedor do serviço e o usuário. Por quê? Por mais que nós tenhamos leis, sabemos que nem sempre a lei é transparente, e às vezes elas guardam coisas que não poderiam estar sendo guardadas.

Uma forma de flexibilizar... Seria muito mais fácil... Eu tive que desenvolver técnicas de forense computacional para poder contornar a grande dificuldade que se tem de rastrear endereços de IPs na Internet. Eu sou capaz hoje de rastrear endereço de IP na Internet com facilidade por causa dessa pesquisa. É um negócio até pouco progressista, mas o fato é que, se flexibilizamos isso, se tiramos do Judiciário esse controle, criamos uma facilidade para o bom policial e para o mau policial. Quem vai ser o juiz disso? Quem guardará o guarda?

É muito sério ter acesso ao dado cadastral de um usuário na Internet pelo endereço de IP. É uma coisa que revela muito da intimidade da pessoa. Se se cria um mecanismo administrativo para isso, cria-se aí um possível mecanismo de abuso severíssimo!

As próprias normas internacionais (ISO 27000, 27001, 27002), que é a série de normas internacionais da ISO que dizem respeito a construir sistemas de gestão da segurança da informação, tudo o que se escolhe em segurança da informação tem que ser pautado no que chamamos de análise de risco. Em relação àquela vulnerabilidade, você vê o risco do qual quer se proteger. Você avalia o quão vulnerável está em relação a ele e qual é o risco de algo acontecer.

O outro ponto que se avalia é o impacto que haverá caso aquilo aconteça. E o terceiro ponto que se avalia é o custo para se proteger. Na minha opinião, é um custo muito alto — espero que as pessoas concordem — flexibilizar tanto a



obtenção de dados pessoais, porque uma coisa é certa: quando é só o endereço IP, eu até discordo que seja dado pessoal.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - Eu queria só fazer um questionamento. O senhor disse que, informando o endereço IP, ia demonstrar muito a intimidade da pessoa, do usuário. Em que sentido isso ocorre? Que intimidade é essa?

O SR. PABLO XIMENES - Por exemplo, ao obter o endereço IP da pessoa, com algumas técnicas, você pode saber as atividades *on-line* dela, pode saber que *sites* ela visita, pode saber que serviços ela usa. Não é difícil fazer isso com técnicas de forense computacional. Isso é só um exemplo. Mas vamos pensar num caso mais concreto. Um policial usa o fato de ter havido um crime contra a honra para receber uma lista de endereços IPs de pessoas que fizeram o registro de reserva em um determinado motel, motel para encontros íntimos. Aí, ele está ajudando, por fora, a esposa que tem um contrato pré-nupcial num caso de divórcio. Ele obtém uma informação de que o marido dela estava no motel tal. Isso conduz a uma investigação que pode resultar num ganho financeiro para a esposa. Enfim, são intimidades que não dizem respeito a uma investigação policial. Não estou dizendo que o policial vá fazer isso, mas cada quebra dessa privacidade tem que passar por uma legislação rigorosa.

A União Europeia já considera endereço IP sozinho como dado pessoal. E há situações rigorosas com relação à guarda dele. Mas, quando se cria um mecanismo puramente administrativo, mesmo que seja só das forças policiais, para se obter endereço IP, começa-se a ultrapassar essa fronteira da qual eu discordo, mas se começa a ultrapassar essa fronteira em relação a dado pessoal. E o endereço IP passa a ser um dado pessoal de verdade. Não vou dizer que sou contra *a priori*. A princípio, acho que tem que haver uma discussão muito mais aprofundada, porque existe um grande risco de abuso.

Se possível, eu queria reservar um momento para poder falar dos outros temas que infelizmente não anotei, para não me alongar demais e comentá-los eventualmente.



O SR. PRESIDENTE (Deputado Rodrigo Martins) - Só peço aos convidados que procurem estender, no máximo, por 5 minutos cada resposta, até porque já estamos com número suficiente no plenário para iniciar Ordem do Dia.

Por ordem de fala, vou passar a palavra ao Sr. Pedro Mizukami.

O SR. PEDRO MIZUKAMI - Sr. Presidente, eu queria agradecer mais uma vez pela oportunidade de participar desta audiência. Fico muito feliz com as perguntas. Todas elas foram muito bem formuladas. Obrigado pela oportunidade de responder a todas. Cheguei a anotá-las aqui, mas, Presidente, queria saber quantos minutos eu tenho.

O SR. PRESIDENTE (Deputado Rodrigo Martins) - São 5 minutos. Está bom assim?

O SR. PEDRO MIZUKAMI - Está bem. Vou tentar responder em 5 minutos.

Em relação à neutralidade de rede, que é a pergunta do Deputado Ronaldo Nogueira, quero dizer o seguinte: todas as questões relativas à segurança, à investigação de crimes, etc., são muito pertinentes, muito sensíveis, muito bem colocadas, mas a neutralidade de rede não é o *locus* adequado para se analisar essas questões. Podemos até entrar em pontos polêmicos que eu mesmo levantei aqui, como a questão da retenção de dados. Podemos tentar fazer essa discussão no contexto de retenção de dados ou no contexto de outras medidas para o combate a crimes ou para reforçar o arsenal existente para investigação de crimes, mas neutralidade de rede não é realmente o *locus*, não é realmente o tópico adequado para fazer estas discussões. A neutralidade de rede é muito mais sobre inovação nas pontas a Internet, é muito mais a respeito de manter condições justas para a competição dos atores que estão neste mercado, para impedir distorções neste mercado e para proteger os direitos dos consumidores. Então, é mais uma questão de infraestrutura, no sentido de executar e no sentido de caminhar em direção a estes valores, a estes ideais.

A discussão sobre segurança é uma outra discussão, e acho que é importante nós destacarmos estes temas do tema da neutralidade de rede, sob pena de acabarmos confundindo as coisas e chegarmos a uma alteração, a uma emenda para o artigo de neutralidade de rede no Marco Civil, que é muito bem formulado,



que seja, no final das contas, como o senhor mesmo colocou, um retrocesso em relação à redação original do Marco.

Eu vejo com bons olhos, evidentemente, reforçar e fornecer todas as ferramentas necessárias para a Polícia Federal proceder às suas investigações, desde que dentro dos limites constitucionais, a investigação penal, desde que dentro dos limites constitucionais para a produção de provas e desde que observados os critérios de necessidade e proporcionalidade que passam pela eficácia da medida e sua adequação aos fins pretendidos. É uma série de análises a que se deve proceder antes de tentar propor esse tipo de solução.

O que eu sempre menciono é que fico muito preocupado quando as soluções propostas são soluções simples demais, porque os sistemas são realmente muito complexos. Por mais que soe plausível, ou que soe interessante exigir um cadastro obrigatório de CPF, eu acho que é importante nós reconhecermos que as crianças são muito mais inteligentes do que isso. É muito fácil você conseguir um CPF. É muito fácil você navegar na rede, caso você tenha essa intenção. E todo mundo foi criança. Acho que todos podem constatar que, quando nos mandam fazer uma coisa, nós sempre levamos em consideração as alternativas para fazer exatamente o oposto.

Então não acho que exigir cadastro obrigatório, CPF, etc., vai resolver algum problema, e acho que os problemas que podem surgir, a partir da exigência desse registro, são muito maiores do que o que nós pretendemos combater com a medida. Quanto mais dados você obriga os provedores a recolher, maior é o potencial de danos que esses dados podem ter, mediante, por exemplo, uma invasão, um vazamento, etc. Então, é sempre importante pensar no princípio de minimização da coleta de dados, coletar exatamente o mínimo necessário para que nós consigamos sobreviver e administrar todos esses problemas que vão surgindo.

Com relação ao Marco Civil da Internet, eu concordo muito com Pedro Markun. Eu acho que é importante dar um tempo de maturação para o Marco Civil da Internet, ver como os tribunais o interpretam. As decisões já estão saindo. Acho importante nós darmos este tempo, este período de respiro para o Marco Civil, para ver exatamente como ele é interpretado e como vai ser aplicado.



Dito isso, acho importante, de novo, considerar qualquer proposta de alteração do Marco Civil no sentido de estar sempre no caminho de necessidade e proporcionalidade das medidas e com estudo muito sério, muito pormenorizado dos potenciais danos e riscos que podemos ter com essas medidas.

Em relação a dados sobre pirataria, nós distribuimos este exemplar do livro que publicamos para vocês. Eu não vou me alongar neste tema, até porque eu tenho 5 minutos, mas eu gostaria de pedir que vocês lessem o que está escrito entre as páginas 103 e 120. São páginas dedicadas exclusivamente a uma análise de pesquisas, em números produzidos pela indústria, e do uso instrumental desses números como estratégia de convencimento. E aqui importa muito menos que os números sejam sólidos, robustos, do ponto de vista estatístico, ou mesmo que haja uma pesquisa por trás.

A exposição do Pablo foi no sentido de criticar números e dados que são produzidos com alguma pesquisa. Às vezes, não existe pesquisa alguma. Esses números são repetidos. Solta-se um *press release*, esse *press release* é repetido *ad infinitum*, e as coisas vão virando verdade. Então, é sempre importante haver um cuidado muito rigoroso com os dados, para saber como os dados são produzidos, se existem dados no sentido contrário, e analisar todo este contexto de provas, de evidências empíricas em relação às políticas públicas que nós estamos defendendo.

Em relação ao PL sobre o tratamento de dados pessoais, estou muito curioso para ver o resultado final da consulta. Comprometo-me a encaminhar, para todos os membros da Comissão, a análise técnica que nós fizemos e que foi entregue ao Ministério da Justiça quando da consulta pública do PL de dados pessoais. Vou encaminhar esse documento, assim como os documentos referentes à consulta do Marco Civil da Internet e o texto que nós preparamos, na FGV, em conjunto com o InternetLab, de São Paulo, e o GPOPAI, da USP, a respeito do PL 215.

Todos esses textos, acredito, têm insumos que podem ser relevantes, que podem contribuir muito para as discussões nesta Comissão, até porque existe uma sobreposição muito grande dos debates que foram travados aqui e dos debates que estão sendo travados em outros fóruns.

Obrigado.



O SR. PRESIDENTE (Deputado Rodrigo Martins) - Passo a palavra ao Markun.

O SR. PEDRO MARKUN - Vou tentar ser telegráfico, porque os senhores já estão com pressa para ir trabalhar, o que faz todo sentido.

Quanto à quebra de neutralidade da Rede: ainda estou para ver uma boa justificativa. Não gosto nem da incisão técnica que nós temos no Marco Civil hoje, perdi essa briga lá atrás. Acho que boa parte das discussões que querem quebrar neutralidade da rede hoje é alguma outra coisa transvestida. Se a pessoa olhar bem, verá que não é preciso quebrar a neutralidade da rede para resolver esses problemas, porque, por exemplo, não é por aí que se vai ou não resolver o acesso da sua filha a conteúdos impróprios. Isso é tentar tapar o sol com a peneira, porque sua filha vai ter sempre outra forma de fazer isso. Eu entendo quando dizem que não podemos ser hipócritas de achar que os pais vão falar com os filhos, mas fico muito triste de entender essa afirmação. Então, já que é para se fazer um decreto que não vai servir para nada, que se faça um que obrigue os pais a conversarem com os filhos e que não tente regular a Internet. Enfim, vocês sacaram, né? É tenso o lance.

O fato é que só se resolve isso com educação. Feliz ou infelizmente, não é uma medida técnica. Isso vem de muito antes da Internet, e eu posso contar vários casos de exposição a conteúdo impróprio da minha infância, não mediada pela Internet. Não há como se resolver isso.

Quanto à guarda de *logs* e à questão de facilitar sem ordem judicial, é muito tenso, mesmo o acesso a IP, enfim, a qualquer informação. Eu já acho difícil — de novo. A ordem judicial, nós já sabemos que ela, no Brasil, serve a quem tem dinheiro. Então, isso já é um problema, mas, pelo menos, há aí toda uma instância, o Judiciário, pensada para resolver esse tipo de conflito, para ver se esse caso, especificamente, vale ou não. Deixar isso na mão da Polícia Federal, com todo apreço que eu tenho à classe, acho complicado.

Dou um exemplo muito prosaico: quando nós resolvemos comprar o primeiro ônibus para o Ônibus Hacker, um amigo meu da Polícia Federal me mandou um *e-mail*: “*Não compre esse, porque o dono tem ficha na polícia*”. Eu respondi: “*Muito obrigado pela informação, mas...*” Vejam o grau de violação da privacidade de um



cidadão, dado o acesso que ele tem, arbitrariamente! E nós vamos dar mais esse monte de informações?

Vão perguntar: “*Mas será que se tem que tirar o acesso à ficha criminal da Polícia Federal?*” Não, mas quando se fala de fluxo de informações da Rede... O Pedro falou um pouco sobre como isso respinga na macropolítica mesmo. São muitas as informações, e o que nós podemos fazer com isso não está no gibi.

O problema — e aí volto à história da Lei de Proteção de Dados Pessoais — é que nós temos uma emergência muito mais premente, que é editar essa lei. Hoje, a Polícia Federal não tem esse acesso, mas o Facebook tem e pode fazer o que quiser com esses dados, inclusive, vender para quem oferecer mais dinheiro. Isso é muito preocupante!

Alguém me enviou uma sugestão ao meu Telegram que eu achei massa de passar aos senhores, Deputados, que é: já que a pessoa vai pedir ao filho, filha, ou primo ajudar lhe a entrar na Internet e conhecer como funciona o uTorrent, existem três séries que vale acessar: *Black Mirror* — especialmente a terceira temporada —, que fala muito de privacidade da Rede, das tecnologias da Rede — é uma série que problematiza isso, e vale acessar ou comprar o DVD, como preferirem; *The Wire*, uma série ainda mais antiga sobre grampo telefônico que problematiza muito a questão do ponto de vista político; e até *Narcos*, com Wagner Moura, que também vale a pena ver.

Narcos tem uma coisa muito louca, porque ela passa ao largo da questão da privacidade, e é tudo muito natural: todo mundo grampeia todo mundo — é uma festa do caqui. Os Estados Unidos pegam informações de todo mundo, e ninguém acha isso muito preocupante. Eu acho! Então, quem ainda não viu *Narcos*, assista e repare em quanta galera que não tem nada a ver com o papo está sendo grampeada por causa de uma investigação. Tudo bem falar: “*Prendam o Pablo Escobar!*” — beleza! —, mas a proporcionalidade disso para quem não tinha nada a ver com o pato é um problema. Grampear o telefone do Pablo Escobar é justíssimo, mas pode haver ordem judicial para isso.

Para finalizar, vamos à questão da pirataria. De novo, eu acho que precisamos de uma revisão da lei sobre direitos autorais. Acho que ela ganha um novo contexto nas redes digitais, mas eu só gostaria de desmentir o Jackie Chan e o



Arnold Schwarzenegger, que, na abertura do DVD, diziam que roubar um filme era a mesma coisa que roubar uma bolsa. Não é, é completamente diferente. Eu não roubo nada da Internet, porque eu não subtraio: o conteúdo continua lá, e todo mundo tem acesso a ele. Eu fiz uma cópia digital, e isso não doeu em ninguém, porque não arranquei pedaço de ninguém. Literalmente, eu fiz uma cópia.

Então, telegraficamente é isso aí.

Uma última coisa sobre educação: eu faço umas oficinas de política, e uma delas se chama *Como fazer um projeto de lei*. Fiz uma delas em Ribeirão Preto, e a grande preocupação das crianças lá — era uma molecada de 11 anos — era o *bullying*.

O *bullying* é uma questão inclusive do ponto de vista das crianças. Eu falei: “O.k., essa é a questão. Qual é a solução?” Elas criaram um projeto de lei com alguns pontos — eu posso até encaminhá-lo para cá, quem sabe vira lei federal: tinha que existir um feriado para discutir a questão do *bullying* na escola, de preferência na quarta-feira, para emendar com o final de semana, e todo mundo tinha que parar com o que estava fazendo, menos bombeiros, policiais e médicos. (Risos.) Mas aquilo de que eu mais gostei — e me arrepio sempre que me lembro — era o quarto ponto da lei: “Os pais precisam conversar com os filhos”. É isso.

Eu entendo a hipocrisia, que não dá para deixar isso por conta dos pais, mas, se não dá para deixar por conta dos pais — talvez precisemos educar os pais —, se não dá para deixar para a escola — na Câmara Municipal de São Paulo, cortou-se do Plano Municipal de Educação o debate sobre gênero e sexualidade —, deixar para a regulação da Internet...

O SR. DEPUTADO RONALDO NOGUEIRA - Presidente, eu não vou aceitar esse tipo de provocação. Os convidados foram tratados com o devido respeito, e eu não vou aceitar esse tipo de provocação. O assunto aqui é crimes cibernéticos, não ideologia de gênero. Por favor, o senhor se atenha ao conteúdo pertinente à discussão.

O SR. PEDRO MARKUN - Está bem. Já que não se pode discutir sexualidade na escola e não se discute sexualidade em casa, acho extremamente complexo tentarmos regulamentar o acesso às informações sobre sexualidade, tecnicamente, na Internet. Acho isso extremamente complexo. A minha posição é: ou resolvemos



isso no campo do diálogo com nossos filhos, e aí cada família tem total liberdade para discutir o assunto como quiser, com total liberdade — pelo menos essa é a minha posição —, ou não vai adiantar. Feliz ou infelizmente, não existe solução técnica para resolver esse problema, estejam em jogo conteúdos que digam respeito à sexualidade, estejam em jogo conteúdos que digam respeito à violência.

Hoje, no avião, estava passando um seriado sobre crime, com pessoas mortas, e a criança ao meu lado estava assistindo àquilo. A televisão mostra gente seminua há anos, e não se consegue regulamentar esse tipo de prática.

Então, desculpem-me, que realmente não era a minha intenção ofender ninguém. Mas faço um apelo para que entendamos que essa legislação, no nível técnico, não vai conseguir resolver esse tipo de problema. Precisamos, sim, puxar essa discussão para o campo educacional.

Mais uma vez peço desculpas, se eu ofendi alguém. Não houve a intenção.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Obrigada.

Concedo a palavra ao Sr. Pedro Rezende.

O SR. PEDRO REZENDE - O que é privacidade? Como pesquisador de segurança na informática, eu me deparei com esse tema de pesquisa. A melhor resposta que eu encontrei foi a de um pesquisador da Universidade Nacional da Austrália. Ele diz que privacidade é a separabilidade de papéis sociais, é a capacidade de o indivíduo escolher como os seus diferentes papéis sociais se comunicam entre si.

O que acontece quando a sociedade evolui para a era da informação, e a tecnologia de comunicação torna transparente, do ponto de vista de quem quer se comunicar, a complexidade envolvida nas transmissões? As pessoas ganham a ilusão de que estão por trás de uma cortina, onde ninguém as vê. E aí, estando despreparadas para a consequência desse alcance maior da comunicação, elas se expõem mais, como se estivessem, por exemplo, circulando na Praça de República de São Paulo às 11 horas da noite sem nenhuma preocupação com possíveis transeuntes. Essa é uma imagem de quem está crescendo com a Internet. E a preocupação dos pais é: *“O que vai acontecer com o meu filho andando na Praça da República às 11 horas da noite, sem preocupação com transeuntes?”*



Então, fica difícil para quem não entende a complexidade técnica de como a Internet surgiu e funciona perceber que as dificuldades de rastreabilidade, identificação, privacidade, etc., na Internet, são o outro lado da moeda de uma coisa que todo mundo acha bom e bonito que é a capacidade praticamente ilimitada de se comunicar. A contrapartida dessa capacidade ilimitada de alcançar qualquer um no planeta é a dificuldade de identificar com quem se está falando.

Na vida em sociedade, nós temos vários canais laterais e canais subliminares para fazer juízo sobre intenção, sobre o contexto cognitivo daqueles com que estamos falando. Quando se vai para uma tela que simula o que é realidade, mas onde o cujo sinal está sendo transmitido de forma eletrônica, vindo ou indo para o planeta inteiro, perde-se a âncora dos canais laterais e não se tem noção do que está acontecendo do outro lado. Tem-se apenas uma vaga ideia.

O filósofo Gilles Deleuze tem uma definição do virtual que eu acho pertinente para estes meus 5 minutos: o virtual não é antônimo de real, nem é sinônimo de irreal; o virtual é a indistinguibilidade entre o real e o irreal. O problema de tratarmos com dados pessoais, do ponto de vista legislativo, é que parece algo que não se consegue definir num parágrafo ou numa justificativa de projeto de lei. Por quê? Porque dado pessoal é um conceito vago de propósito, por sua natureza subjetiva. Se não se entender a diferença entre dado e informação, não se consegue entender o que é dado pessoal. Informação é aquilo que o dado representa quando ele encontra um contexto cognitivo onde ele se torna capaz de transmitir alguma mudança de conhecimento a respeito da sua origem.

Então, o que é identidade? Também fui buscar algum pesquisador que pudesse me esclarecer essa confusão da Internet. Identidade, para Muniz Sodré, é um corte, uma projeção em algo que é, ou parece ser, o mais estável possível no indivíduo. Então, todo mundo pensa que identidade é o nome que está no registro civil, porque é algo que normalmente não se muda, assim como o RG e o CPF.

Qual o problema de colocar uma chave criptográfica para identificar uma pessoa na Internet e ter a rastreabilidade que se teria, por exemplo, dentro de casa, dentro do escritório, dentro da empresa? É que, para fazer isso, ainda não se venceu o último passo do rastreamento: a conexão entre a máquina e a pessoa. A máquina está rodando *software* que tem 3 mil bibliotecas que o usuário comum não



sabe por que estão ali. A possibilidade de essa máquina estar jogando coisas no seu HD sem que ele veja ou saiba... Ele não sabe o motivo, mas abrir uma janela de uma página na Web pode chegar ao ponto de deixar a máquina ingovernável.

É impossível atribuir responsabilidade a uma pessoa porque ela está usando um IP dentro do ordenamento jurídico de equilíbrio de riscos e responsabilidades, com amplo direito de defesa, como temos hoje. Então, se se quer vencer esse passo entre a identificação de uma máquina e a identificação de uma pessoa para responsabilizá-la com relação ao que a máquina está transmitindo e recebendo, só há uma saída: implantar um *chip* eletrônico debaixo da pele, na testa ou na mão da pessoa. Quem conhece as profecias do *Apocalypse* sabe em que isso vai resultar.

Este é o problema de dar poder demais à Polícia Federal para investigar. Se a Polícia Federal, ou qualquer outra no mundo, está tendo trabalho demais para investigar, isso tem a ver com o fato de que a comunicação hoje é global e instantânea. Não existe nenhuma obrigação de a tecnologia que oferece essa comunicação oferecer uma solução para os problemas que surgem. Ela está oferecendo o problema.

Se a queremos oferecer uma solução para quem deveria estar cuidando, em nome do Estado, da ordem social e da ordem pública... Estamos criando uma solução que, quando a escassez chegar, quando o desabastecimento chegar, quando a crise econômica e financeira atingir um nível crítico, vai se transformar numa coisa irreconhecível e sem controle: o Estado soberano, totalitário e global controlado por aqueles que detêm a infraestrutura de comunicação digital planetária.

Então, é um risco muito grande querer solução técnica para um problema de natureza semiológica.

Vou passar ao largo da questão da responsabilidade na criação dos filhos e tentar encerrar com uma metáfora. Eu estava numa conferência de CryptoParty, em São Paulo. Saindo de uma palestra, indo para um restaurante, uma pessoa que estava na plateia estava caminhando do meu lado. Eu não sei o nome, mas quero lhe dar o crédito da metáfora que achei muito interessante. Disse ela que dado pessoal é como matéria radioativa: na natureza, é inofensiva onde está, mas, a partir do momento em que é concentrado, começa a produzir reações em cadeia capazes de tirar o sossego das pessoas.



O que é tirar o sossego das pessoas? No momento em que quem controla o uso da tecnologia digital no planeta tiver condições, como faz o governo americano, de planejar ataques com *drones*...

Vinte por cento dos ataques de *drones* no Paquistão, em 2012, foram programados sem identificação positiva do alvo. O alvo era escolhido por mineração de dados, por tráfego em redes sociais e por GPS, segundo o lugar por onde o *chip* do celular da pessoa andava. “*Esse cara tem o perfil de alguém que é perigoso porque retuíta mensagens com essas, essas e essas palavras, e ele anda por esses, esses e esses lugares dessa região. Então, bomba nele!*”. E isso sem saber quem é a pessoa.

Pois bem, no momento em que a geopolítica chega a esse ponto de usar dados minerados, torna-se um perigo liberar dados que, quando colocados juntos com dados pessoais — endereço, telefone, número de IP, etc. —, provocam reações em cadeia que empoderam quem controla a capacidade de agregar dados para gerar informações pessoais.

Esse é o problema para o qual eu quis alertar com a minha palestra sobre flexibilizar ou gerar exceções para os princípios basilares que procuraram ser consolidados no Marco Civil como princípios de direitos pessoais e universais. Senhores, tecnologia digital, tecnologia da informação, hoje, é instrumento de exercício do poder político. Se isso escapar à percepção dos senhores, o risco de fazerem leis que explodam lá na frente em seus efeitos colaterais é muito grande. Então, peço aos senhores atenção redobrada para os *lobbies* nesta Casa, em se tratando de legislação de tecnologia digital.

Muito obrigado pela atenção.

A SRA. PRESIDENTA (Deputada Mariana Carvalho) - Nós é que agradecemos, mais uma vez, a presença e a participação de todos, as contribuições dadas a esta Comissão, sobretudo porque sabemos da agenda dos senhores.

Obrigada por estarem aqui, porque é necessário o amplo debate que estamos tentando ter com os vários segmentos, com vários pensamentos, com várias opiniões. É assim que se constroem os andamentos da CPI.

Quero, mais uma vez, solicitar os materiais e as sugestões que possam ser encaminhadas ao endereço eletrônico da Comissão. São importantes para, junto



com nossa consultoria, ouvirmos e avaliarmos o que trazem os senhores, que têm história com o tema.

Agradeço, por fim, o livro que ganhamos de presente.

Como disse o Deputado Odorico, o tema foi muito debatido nesta Comissão, na semana passada, mas ainda é muito cedo para dizer como serão os andamentos da CPI. Nosso Relator e nossos Sub-Relatores vão estar à frente desse amplo debate.

Nada mais havendo a tratar, declaro encerrada a presente reunião, antes convocando reunião ordinária para a próxima quinta-feira, dia 15 de outubro, às 9h30min da manhã.

Está encerrada a reunião.