



DEPARTAMENTO DE TAQUIGRAFIA, REVISÃO E REDAÇÃO

NÚCLEO DE REDAÇÃO FINAL EM COMISSÕES

TEXTO COM REDAÇÃO FINAL

*Versão para registro histórico*

*Não passível de alteração*

COMISSÃO DE SEGURANÇA PÚBLICA E COMBATE AO CRIME ORGANIZADO			
EVENTO: Audiência Pública	REUNIÃO Nº: 1373/16	DATA: 09/11/2016	
LOCAL: Plenário 6 das Comissões	INÍCIO: 16h16min	TÉRMINO: 17h02min	PÁGINAS: 16

DEPOENTE/CONVIDADO - QUALIFICAÇÃO

PABLO BARCELLOS BERGMANN - Representante da Polícia Federal.  
CARLOS BRUNO FERREIRA DA SILVA - Procurador da República, representante da Procuradoria-Geral da República.

SUMÁRIO

Debate sobre a forma, os prazos e os meios de preservação e de transferência de dados informáticos, em posse de fornecedor de serviço, a autoridades públicas, para fins de investigação criminal com envolvimento de delito contra criança ou adolescente, nos termos contidos no Projeto de Lei nº 2.514, de 2015.

OBSERVAÇÕES

Houve exibição de imagens.  
Há palavra ou expressão ininteligível.



**A SRA. PRESIDENTA** (Deputada Laura Carneiro) - Esta audiência foi convocada para debatermos a forma, os prazos e os meios de preservação e de transferência de dados informáticos, mantidos por fornecedor de serviço, a autoridades públicas, para fins de investigação criminal envolvendo delito contra criança ou adolescente, nos termos do Projeto de Lei nº 2.514, de 2015, em atendimento ao Requerimento nº 173, de 2016, de autoria da Deputada Laura Carneiro, que relata a matéria.

Convido para comporem a mesa os Sr. Pablo Barcellos Bergmann, representando o Departamento de Polícia Federal, e o Exmo. Sr. Dr. Carlos Bruno Ferreira da Silva, Procurador da República, representando o Sr. Procurador-Geral da República.

Cada convidado disporá de 20 minutos para sua exposição, vedados os apartes, tempo que poderá ser estendido, de acordo com o interesse da reunião. Os Deputados interessados em interpelar os convidados deverão inscrever-se previamente junto à Secretaria.

Concedo a palavra ao Sr. Pablo Barcellos Bergmann, representante da Polícia Federal.

**O SR. PABLO BARCELLOS BERGMANN** - Boa tarde.

Vou rapidamente passar alguns conceitos sobre a pornografia infantil e a atribuição da Polícia Federal, porque sempre há muita confusão sobre esses temas. Em seguida vamos entrar no mérito do projeto de lei.

É comum se utilizarem os termos “crime de pedofilia”, “vamos combater a pedofilia”. Na verdade, pedofilia não é crime, é um transtorno, uma psicopatologia, como é voyeurismo, fetichismo, etc., caracterizada pela preferência sexual por crianças. Então, o fato de ser portador desse transtorno não quer dizer que seja um criminoso. Ele pode ser externado a partir de condutas criminosas ou não.

A pornografia infantil seria a representação de uma criança envolvida em atividades sexuais explícitas ou a representação dos órgãos sexuais de uma criança ou adolescente. Essa é a definição do Estatuto da Criança e do Adolescente. Então, para existir pornografia infantil, tem que existir representação. Obviamente, a pornografia infantil está de alguma forma ligada ao abuso sexual de criança ou



adolescente. Ela não é o abuso, é a representação, normalmente através de imagens ou vídeos, de um abuso.

Qual é a atribuição da Polícia Federal sobre essa matéria? Ela advém do art. 109, inciso V, da Constituição Federal, que diz:

*“Art. 109.....*

*V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente.”*

Mas onde entra a pornografia infantil? O Brasil é signatário da Convenção sobre os Direitos da Criança, tratado internacional que prevê que os países reprimirão os crimes de pornografia infantil. Então, a primeira premissa, crime previsto em tratado ou convenção internacional, está suprida com a existência da Convenção sobre os Direitos da Criança, da ONU.

A segunda parte diz *“tenha ou devesse ter ocorrido no estrangeiro”*, é chamada de *“transnacionalidade”*. Então, não é todo crime. E é muito comum ouvir: *“Basta a utilização da Internet para caracterizar a transnacionalidade”*. Sempre existe certa confusão em relação a isso. *“Ah, Internet é Polícia Federal”*. Não é bem assim que funciona. Não necessariamente a utilização da Internet caracteriza que houve resultado que tenha ou devesse ter ocorrido no estrangeiro.

Se eu envio uma mensagem do Brasil para algum usuário que está aqui, em momento algum houve resultado fora do País. Então, não são todas as formas de utilização da Internet que caracterizam a transnacionalidade. Isso foi objeto de recurso extraordinário julgado pelo Supremo Tribunal Federal no ano passado, cujo número está aqui.

Na verdade, a maioria dos casos é de competência estadual, não federal. Evidentemente, isso não impede a Polícia Federal de atuar quando as coisas estão conexas. Por exemplo, um abuso sexual, que é de competência estadual, foi registrado e enviado para fora do País. Evidentemente, nós podemos investigar toda a conduta, desde o início, e responsabilizar os autores.



Na Polícia Federal, normalmente, São Paulo, Minas Gerais, Bahia e Rio de Janeiro são os Estados que têm mais investigações em andamento nessa área. Só São Paulo tem mais de 800.

Vamos, então, ao projeto de lei, nosso objeto hoje, o que nos interessa. Eu notei que, apesar de ter recebido como ano de apresentação 2015 na Câmara dos Deputados, ele é originário do Senado, de 2008. Não é isso, Deputada?

**A SRA. PRESIDENTA** (Deputada Laura Carneiro) - Na verdade, foi votado e aprovado no Senado com esse texto. A grande discussão seria: até que ponto é justo que a Polícia Federal acesse diretamente IP e dados sem passar pelo Poder Judiciário? Essa tem sido uma premissa em todas as instâncias em que votamos o tema na Casa.

**O SR. PABLO BARCELLOS BERGMANN** - Ótimo. Sem dúvida, esse é o cerne da questão, o ponto que prejudica bastante as investigações, e que, enfim, beneficiaria as investigações criminais.

Ocorre que, pelo fato de o projeto ser anterior ao Marco Civil da Internet, as definições que ele traz... Este projeto de lei chama de “fornecedor de serviço”, que seria equivalente a “provedores” no Marco Civil. Então, como este projeto de lei e o Marco Civil estão tratando das mesmas entidades, essa dualidade de definições são díspares em alguns pontos, e é uma coisa que dificultaria sua aplicação na prática, na redação em que se encontra hoje.

Só para exemplificar alguns pontos muito evidentes, por exemplo, a definição de “fornecedor de serviço de conteúdo interativo” seria o equivalente a “provedor de aplicação” do Marco Civil. A definição que está no projeto de lei não é muito adequada, do meu ponto de vista. Ela poderia deixar de fora situações vitais para uma investigação.

**A SRA. PRESIDENTA** (Deputada Laura Carneiro) - Com a nomenclatura, não se preocupe.

**O SR. PABLO BARCELLOS BERGMANN** - Então vamos ao que interessa.

**A SRA. PRESIDENTA** (Deputada Laura Carneiro) - Na verdade, o objetivo da audiência pública é tratar do cerne da questão, até porque, depois do Marco Civil, aprovamos, na CPI dos Crimes Cibernéticos, vários outros projetos de lei. É óbvio



que vai ter que se adequar tudo isso. Esqueça as nuances, que são facilmente sanáveis. Vamos para os temas principais.

**O SR. PABLO BARCELLOS BERGMANN** - Ótimo.

Então, no principal, o que há de alteração é que passa para 3 anos o prazo de guarda. Isso é ótimo. Realmente, já estamos tendo problemas com esse prazo de guarda de 1 ano. Alguns provedores passaram a excluir as informações após esse período. Apesar de no Marco Civil não existir essa obrigação na publicação do decreto que o regulamentou, ele trouxe uma redação que obrigou os provedores a excluírem após 1 ano. Na redação dá para entender isso, e alguns já começaram a fazer. Se se pede algum mandado...

*(Intervenção fora do microfone. Ininteligível.)*

**O SR. PABLO BARCELLOS BERGMANN** - Exato, ele responde que não tem, apesar de muitos ainda guardarem por 3 anos, até em razão de termo firmado na época da CPI da Pedofilia, em 2008, quando os provedores foram obrigados a guardar por 3 anos. Então, essa alteração para 3 anos seria excelente.

Em relação à requisição direta dos dados pelo Ministério Público e pelo Delegado de Polícia Federal, tenho artigo escrito sobre o tema, cuja cópia vou deixar com a Sra. Deputada e com o Dr. Carlos Bruno, desmistificando que isso seria violação de intimidade, etc., porque os *logs* de IP, os registros de acesso às conexões não trazem nenhum dado que sequer identifique a pessoa responsável por aquela ação. Ela simplesmente permite que se identifique uma conexão de Internet. Seria o equivalente a uma placa de carro — não se consegue identificar quem estava dentro do carro, muito menos para onde ele foi e o que fez.

A exigência de ordem judicial para a obtenção desses dados é um dos fatores que mais atrapalham a investigação de crimes cibernéticos hoje. Então, essa alteração seria de enorme valia para a persecução penal, e, mais ainda, o estabelecimento dos prazos, também uma medida excelente, especialmente a do caso de risco eminente à vida, de 2 horas, ou 12 horas, quando houver risco à vida.

Isso está inclusive fazendo alinhamento com a legislação, especialmente americana, na qual já existe essa previsão. As grandes empresas — Facebook, Google, Yahoo, etc. — já têm uma estrutura preparada para isso, basta apenas que o Brasil aprove esse normativo, para legalizar a obtenção desses dados. Essas



empresas já possuem essa estrutura porque nos Estados Unidos é interesse da empresa fornecer esses dados para evitar a violência física, o abuso, a uma criança, a morte de uma pessoa. Isso, sem dúvida, é de enorme valia.

Outra parte também muito interessante é a que prevê as punições, que o Marco Civil não previu, e as empresas não cumprem esses prazos e fica por isso mesmo. Eu acredito que a regulamentação do processo para apurar a punição que diz respeito a esses prazos também é interessante.

Então, do ponto de vista da persecução penal, o cerne do projeto, o mérito dele em si, que é a possibilidade de obtenção dos dados de conexão e o estabelecimento de prazos, é excelente. É a opinião minha e da Polícia Federal.

Obrigado, Deputada.

**A SRA. PRESIDENTA** (Deputada Laura Carneiro) - Obrigada, Dr. Pablo.

Vamos ouvir o Dr. Carlos Bruno Ferreira da Silva, Procurador da República, representando a Procuradoria-Geral da República.

Peço aos senhores que deixem as apresentações para a Comissão.

**O SR. CARLOS BRUNO FERREIRA DA SILVA** - Boa tarde a todos. É um prazer estar aqui.

Em primeiro lugar, saúdo a Relatora e Presidenta da Mesa, Deputada Laura Carneiro, filha do saudoso Senador Nelson Carneiro, a quem, denunciando minha idade, dei meu primeiro voto. O Senador Nelson Carneiro, do meu Estado natal, é um político muito saudoso do Rio de Janeiro.

Saúdo também meu companheiro de Mesa, Delegado Pablo Bergmann, que fez uma palestra belíssima, conhecedor que é do tema — trabalha com o assunto. Realmente foi muito boa, porque tratou do projeto de lei e apontou uma questão que também acho relevante, sua compatibilidade com o Marco Civil.

Faço meu elogio a este momento. Pelo visto, vou falar um pouco além do que a Deputada pretendia, porque me parece um ótimo momento, uma ótima discussão no Parlamento. Sempre fico muito feliz em estar em audiências públicas da Câmara dos Deputados. Quando vou para o trabalho na Procuradoria-Geral da República, às vezes vou ouvindo no rádio as audiências públicas. Realmente é muito o conhecimento que se passa por aqui, demonstrando a seriedade com que o Parlamento trata a edição de normas.



Como já participei de algumas audiências, vim para esta com o objetivo de passar um pouco os problemas que, pelo menos do ponto de vista do Ministério Público Federal, temos encontrado nos crimes cibernéticos em geral. Faço minhas as palavras do Delegado Pablo: também faço sempre a conceituação teórica de que não tratamos de pedofilia, mas sim de pornografia infantil e de abuso de menores; pedofilia é uma doença, abuso de menores e pornografia infantil são crimes. Então, vamos um pouco além.

Esse é um foco do MPF, que tem um grupo de trabalho só sobre pornografia infantil. Há uma atenção nossa muito grande. Ao mesmo tempo — até conversando com o Delegado Pablo verifiquei que é assim também na Polícia —, há uma preocupação mais ampla quanto aos crimes cibernéticos em geral, até porque, cada vez mais, a criminalidade que é atendida pela Polícia Federal e pelo Ministério Público Federal se utiliza de computadores, iPhones, aplicativos para cometer crimes. É cada vez mais difícil essa investigação em razão do uso desses aparatos, desses aplicativos, por se esconderem nas possibilidades da Internet.

O começo da minha palestra tem o objetivo de mostrar como cada vez mais nossa vida é virtual. Isso todo mundo sabe. Nós usamos isso a Rede a todo o tempo. Certamente, no futuro haverá problemas na coluna das pessoas por ficarem com a cabeça baixa, olhando para seus iPhones. Na nossa vida, passamos muito tempo fazendo isso, lidando com as pessoas do nosso convívio via Facebook, WhatsApp, Telegram, *e-mail*. Então, nossa vida cada vez mais é em computadores e iPhones, que na realidade é um computador diminuto, utilizado também como celular: não é um celular utilizado como computador, é um computador que também faz as funções de celular. Evidentemente, a criminalidade também se utiliza desses que são meios usuais de comunicação.

A grande questão — neste momento ainda é um pouco vantagem para os órgãos investigadores no mundo inteiro — é que o computador e a Internet dão uma falsa sensação de anonimato. Quando se está utilizando a Internet, a maior parte das pessoas, até mesmo as que trabalham com isso, como o Delegado Pablo, esquece que aquilo é altamente invasivo. É verificado.

Lembro que o próprio Zuckerberg, dono do Facebook, tem, na parte da câmera do seu *notebook*, um adesivo para não ser utilizado. Não uso no meu, mas



já me prometi que vou usar. O fato é este: quando se usamos a Internet, apesar da falsa sensação de anonimato, estamos abertos a todo tipo de verificação, a começar pela primeira, nosso IP, nosso registro de acesso, que identifica quem somos. Cada vez que acessamos será, em tese, possível verificar como estamos acessando.

Eu estava conversando com o Delegado Pablo. Já trabalhei muito com IP, data e hora para verificar o usuário. Hoje em dia os aplicativos têm dados de geolocalização — os metadados dentro do uso dos aplicativos.

O Marco Civil, de alguma forma, tangencia pontos de interesse para a investigação criminal quando regula a guarda de registros, tanto ao tempo quanto às obrigações do provedor de acesso, de conexão, de serviço, de aplicação, de conteúdo, qualquer nome que se dê. Está tratando de temas que interessam às forças de segurança. Na realidade, é muito normal que entendamos dessa forma, até porque o Marco Civil fala exatamente nesses artigos em Polícia Federal e Ministério Público poderem acessar dados cadastrais.

Então, são normas de natureza penal dentro do Marco Civil. No entanto, ele não é, não foi pensado como norma penal. Como também atuo na parte de consumidor, no Ministério Público Federal, eu me reuni por várias vezes com o Deputado Alessandro Molon, Relator do projeto, e em nenhum momento se pensava diretamente na questão criminal. Ela fazia parte da discussão do Marco Civil, mas não era central nessa discussão. Então, repito, vem em muito boa hora uma discussão sobre a parte penal da investigação de crimes cibernéticos.

Vou falar de crimes cibernéticos em geral. Porém, evidentemente, ao que mais se dá atenção, inclusive nos Estados Unidos, é pornografia infantil: primeiro, pela facilidade que a Internet deu para a transmissão de pornografia — pornografia em geral, em especial pornografia infantil; segundo, pelo dano que ela causa, pela sua gravidade. Vários estudos, também dos americanos, que dão grande atenção ao tema, apontam que o indivíduo que comercializa pornografia infantil é potencialmente um agressor sexual. No fundo, há simplesmente algum limite no superego dele que ainda o impede, mas ele tem todo o substrato mental para ser um agressor sexual.

Vou tentar falar de coisas sobre pornografia infantil que se aplicam a todos os crimes cibernéticos, porque, como eu disse, vários crimes em que Ministério Público





Federal e Polícia Federal atuam são feitos ou combinados via computador, iPhone, Android, o que for. Hoje em dia vemos muito isso na cooperação internacional — e recebo muitos pedidos. Então, há realmente interesse em saber como podemos atuar melhor nesses pontos.

*(Segue-se exibição de imagens.)*

O primeiro problema que temos verificado na investigação de crimes cibernéticos, letra A, é a informação, pelo provedor de conexão, de múltiplos IPs. Vou falar deste assunto rapidamente, em homenagem à plateia e devido ao tempo, e até porque é maçante, técnico. Antigamente, quando havia IPv4 para todos, cada usuário no Brasil tinha um IP separado.

O problema é que a transição de IPv4 para IPv6 ainda não ocorreu. Quando houver IPv6, este outro cenário vai ocorrer novamente. Mas enquanto houver essa transição, os provedores de acesso, para não terem que negar acesso a algum usuário brasileiro, para permitirem que a população continue acessando a Internet, são obrigados a dar mais de um endereço de IP para o mesmo usuário. Com isso, por vezes, quando Polícia Federal ou Ministério Público Federal pede informação aos provedores de conexão, vem no mesmo IP mais de um usuário.

Isso, para crime em geral, não é problema. Por exemplo, crime de pornografia infantil. A pessoa que gosta de pornografia infantil vai ter acessado tantas vezes, que simplesmente vamos fazer um conjunto e verificar que seu nome aparece sempre. Os outros que aparecem não são os investigados.

No entanto, em crime como terrorismo, situação mais urgente, pode causar algum problema ter que se verificar isso num tempo muito curto. Sugestão que surgiu durante um fórum em São Paulo do Comitê Gestor da Internet — CGI, tanto da Polícia Federal quanto do Ministério Público Federal, foi que também o provedor de conexão tivesse que anotar a porta de acesso. Mesmo que o IP seja comum, as portas serão diferentes. A obrigação de guardar a porta de acesso facilita a indicação, permitindo novamente a identificação unívoca do usuário.

Evidentemente, os provedores de conexão não querem fazer isso. Apesar de eu estar falando de 1 byte, cada dado custa muito. Imagine milhões e milhões de acessos. Isso custa dinheiro. Então, naturalmente, eles têm resistência em não fazer. Seria um assunto para termos atenção.



Outro assunto que saiu em toda a mídia é a recusa de fornecimento — vou falar primeiro de metadados, depois de conversas —, causando o bloqueio do WhatsApp três vezes.

Em primeiro lugar, entendo que o art. 11 do Marco Civil obriga os provedores de aplicação no Brasil a cumprirem as ordens da Justiça brasileira. Não tenho dúvida de que o art. 11, que dispõe sobre a jurisdição brasileira, obriga a cumprir.

Dentre as informações que os provedores de aplicação podem fornecer, especialmente de comunicação, que acabam sendo o foco principal nas investigações de crimes cibernéticos porque funcionam um pouco como antes era a interceptação telefônica, tão importante para a elucidação de tantos crimes, dentro da comunicação cibernética existe a possibilidade de verificar os metadados — IP, hora de acesso, localização — e o conteúdo da conversa.

Vou começar pelos metadados, porque o conteúdo da conversa tem o problema da criptografia ponta a ponta. Dentre os metadados, eu entendo, apesar de o Facebook afirmar que é necessária a cooperação internacional, que o art. 11 permite pedido direto ao Facebook no Brasil, feito dentro da norma do Marco Civil, mediante ordem judicial. Por isso, na minha apresentação repito essa questão da ordem judicial, que a Comissão, é claro, vai ter tempo para avaliar.

Dentro do Marco Civil, dentro da norma atual, eles são obrigados a cumprir esse tipo de decisão, apesar de afirmarem que é necessária a cooperação internacional. Há uma proposta do MRE de mudar o tratado do Brasil com os Estados Unidos, para que ele tenha um *fast track*, uma situação simplificada para crimes cibernéticos. Por quê? Porque em crimes cibernéticos a cooperação não pode ser longa, porque prova de crime cibernético é naturalmente volátil, fácil de destruir com o tempo. Então, o ideal é que se cumpra aqui. Eu acho que o Marco Civil permite esse cumprimento.

Minha primeira proposta seria reforçar o mandamento do art. 11 do Marco Civil, exigindo que qualquer provedor de serviço, aplicação, conteúdo que atenda o mercado brasileiro cumpra, seja obrigado pela jurisdição brasileira.

Parece-me que esse argumento de que o servidor está em outro país é falacioso e digo por quê. Primeiro porque o servidor não está nos Estados Unidos, está em um lugar de custo mais baixo, normalmente em alto mar, dividido. A



navegação em nuvem permite que a informação se divida e só se una quando pedida. A sede está nos Estados Unidos, mas isso também não é desculpa, e digo por quê.

Itaú e Banco do Brasil têm filiais no Paraguai. Já imaginaram se um procurador paraguaio pedisse a quebra de sigilo bancário e o Itaú dissesse que não fornece os dados bancários porque estão armazenados no Brasil? Seria uma loucura. E também o contrário: imaginem se pedíssemos quebra de sigilo bancário ao Santander e ele dissesse que os dados dos clientes brasileiros são guardados num provedor na Argentina, por ser mais barato? Imaginem dizer que não cumpre? É o mesmo argumento.

Apesar de o Facebook ter sede no Brasil, eles argumentam que não vão cumprir nossa decisão porque o servidor está fora, a sede está fora. Os bancos poderiam fazer a mesma coisa. Existe jurisprudência americana dizendo que isso não pode. Por quê? Porque o Facebook, da mesma forma que, no Brasil, afirma que tem sede nos Estados Unidos, para certos dados que o DOJ — Departamento de Justiça pede ao Facebook, ele afirma que tem sede na Irlanda. Ele vai se livrando.

Quanto ao fornecimento de conversas, existe a criptografia ponto a ponto, que é uma técnica utilizada, inclusive pelo próprio *e-mail* da Procuradoria da República. Há colegas que entendem que a criptografia ponto a ponto viola a Constituição. Eu tenho dificuldade de ver dessa forma. Sei que Polícia Federal e Ministério Público Federal trabalham com isso, e obviamente não vou entrar em detalhes. O que podemos tentar é utilizar tecnologias ou técnicas investigativas que nos permitam acessar conversas. Para tanto, é importante que haja norma expressa exigindo o apoio do provedor de conexão e do provedor de aplicação.

Novamente entro no mérito da ordem judicial. É importante que se diga que quando houver justificativa para a atuação criminal, em prol do interesse público, os provedores de conexão e de serviço são obrigados a nos apoiar no cumprimento dessa ordem, na técnica que o juiz chancelou por meio da medida cautelar, permitindo-nos esse tipo de técnica investigativa.

Quanto à recusa de cumprimento de ordem judicial brasileira, entendo que a melhor tática não é bloquear. Aliás, a história comprovou que não é: o WhatsApp continua não cumprindo; serviços públicos e Municípios pequenos saem afetados, porque vários Municípios pequenos se utilizam do WhatsApp para fazer



comunicações; a população como um todo se vê afetada; em poucos dias isso cai, porque não há como bloquear o WhatsApp para sempre.

A melhor solução para obrigar o cumprimento de ordem judicial é clássica: envolver o bolso. Essas empresas têm um faturamento enorme no Brasil. Têm um faturamento enorme! Elas serão afetadas se se bloquear esse faturamento com a aplicação de multa diária até que cumpra a decisão. É a melhor forma de cumprir e não afeta a população, só a empresa que se recusa a cumprir a jurisdição brasileira.

No entender do MPF essa é a melhor estratégia e já a utilizamos em alguns processos. Mas exatamente por falta de norma expressa permitindo aplicação de multa diária nesse caso, há jurisprudência contrária, dizendo que é só no fim do processo. Aí, claro, não funciona. Se se aplicar multa diária e não se puder cobrar imediatamente, se tiver que esperar o final do processo, evidentemente, num caso de crime cibernético, que exige resolução rápida, isso não vai funcionar.

Outra questão que verificamos — e acabei de verificar que está no projeto — é a possibilidade de perecimento da prova. É importante — e a Polícia Federal faz um trabalho excepcional nesse ponto com a *(ininteligível)* 24/7 — que, sendo órgão da Justiça brasileira, sendo cooperação internacional, possamos logo pedir a preservação da prova, avisar ao provedor de serviço que, por mais que favoreça a privacidade do seu usuário, não é cúmplice do crime.

É importante poder dizer: *“Olha, temos a suspeita de que é um crime cometido. Você está me dizendo que precisa de determinada coisa para me dar a prova. Tudo bem. Não precisa me dar agora, mas mantenha a prova — mas mantenha a prova”*. É importante fazer isso com muita celeridade. E li até que o projeto já fala por escrito. Até fiz a sugestão, enquanto escrevia esta apresentação, de que pudéssemos fazer isso por *e-mail*.

Estou com um caso, por exemplo, em cooperação, que envolve o *site* de vídeos pornográficos Xvideos. E todos esses *sites* têm um serviço de atendimento ao usuário, que responde. Por acaso, até o serviço de atendimento ao usuário do Xvideos cita a Polícia Federal — até liguei para o senhor — e diz que aceitaria pedido seu para preservação de prova.

É importante que nossa legislação também garanta que Polícia Federal e Ministério Público possam — inclusive está no projeto — evitar esse perecimento da



prova. Depois, pedimos ordem judicial para acessar a prova, vemos como fazer para acessá-la. Mas não a destruam, porque muitas vezes isso é feito em minutos.

Em relação aos crimes cibernéticos, o projeto é muito feliz quando dispõe que, em alguns casos, em 2, 5 horas tem que ser fornecido. O projeto é muito feliz. A celeridade em crimes cibernéticos é fundamental. Então, o projeto faz muito bem em se preocupar com essa questão do perecimento.

Além disso, isso é importante, na cooperação internacional e no Ministério Público Federal como um todo, também temos investigado outras questões. Isso envolve muito a Polícia Federal, que recebe muita informação de órgãos estrangeiros — FBI, polícia da África do Sul, polícia da Austrália — sobre cometimento, grupos na *deep web* que agem trocando pornografia infantil, que envolve brasileiros.

Obviamente, a atuação da Polícia Federal é muito mais efetiva do que a polícia da África do Sul emitir ordem de prisão para esse caso. Houve um caso de médicos em uma cidade do interior, cujo nome não vou falar, de um Estado grande do Brasil, em que a atuação tinha que ser rápida, muito célere. Não havia como o FBI fazer cooperação internacional, mandar via DOJ, passar pelo DSI — Department of Special Investigation a comunicação do crime que estava sendo cometido, e mandaram diretamente para a Polícia. Instauraram inquérito e rapidamente prenderam esses médicos. Qual é o problema? A defesa alegou que a prova era nula, tinha entrado no Brasil sem seguir o procedimento via autoridade central. Isso não é problemático. Vários países europeus têm cooperação direta em casos urgentes. Aliás, nesse caso de pornografia infantil, pela gravidade do crime, a jurisprudência da 1ª e da 4ª Região — já houve três casos com isso — é de que a prova é válida, de que esse tipo de cooperação é possível.

Para dar segurança à atuação da Polícia Federal, entretanto, é importante que isso esteja expresso na legislação. É importante que esteja expresso. No caso da cooperação direta em casos urgentes, pode se prescindir da passagem via autoridade central, que, repito, é situação que ocorre costumeiramente. O problema é que um dia um desembargador vai dizer que essa prova é nula. E aí nós vamos perder uma operação.

V.Exa. quer que eu acelere a apresentação, para terminar?



**A SRA. PRESIDENTA** (Deputada Laura Carneiro) - Não. Eu quero que mande para mim as duas decisões do TRF.

**O SR. CARLOS BRUNO FERREIRA DA SILVA** - Mandarei.

Há outra questão importante, e de novo me inspiro na dilação americana. Nós temos muita informação, e a Polícia Federal tem um ótimo contato com as autoridades americanas, continua recebendo informações do The National Center for Missing and Exploited Children — NCMEC. Mas seria importante que tivéssemos procedimento similar no Brasil. Explico o que é e como funciona.

Na realidade, esses *sites*, ainda mais Google, Facebook, os buscadores, têm robzinhos que se chamam *bots*, que ficam correndo na Internet, buscando informações para os buscadores. Enquanto estão buscando essas informações, eles se deparam com *hash* de fotos que envolvem pornografia infantil. Isso é muito comum. Eles conseguem ver isso. Quando o robzinho verifica que há pornografia infantil, a legislação americana exige que esses provedores informem a um órgão americano. Esse é o estilo americano. O NCMEC é uma ONG, porque é público e privado — tem fornecimento público, mas é privado —, que recebe essas notícias-crime e as distribui pelos Estados Unidos.

Obviamente, eles encontram também coisas de outros países. No caso do Brasil, mandam para cá. Mas seria importante haver norma similar aqui, até para acelerarmos isso e não haver dúvidas depois sobre o procedimento. Mandam direto para a Polícia. Isso é muito interessante, tem até a ver com a discussão sobre Acordo de Leniência.

Eu estive há pouco tempo na Inglaterra, pela Cooperação Internacional. Um advogado inglês disse que a legislação inglesa de Acordo de Leniência não pensa mais que polícia e ministério público têm que ficar dentro das empresas verificando se houve corrupção ou não. Eles exigem das empresas que elas tenham programas de *compliance* e, dentro desse programa de *compliance*, informem às autoridades que está ocorrendo crime. A empresa, assim, não vira ré, vira, na realidade, parceira do Estado no desfazimento de crimes. Não é interesse da empresa acreditar nisso. Eu acho que esse vai ser o futuro do Brasil.

Eu estive há pouco tempo num evento sobre *compliance* em São Paulo. Todas as empresas — a Odebrecht estava presente — afirmam isso com toda a



clareza. Elas querem trabalhar dentro do mercado capitalista. Ou seja, no futuro — que também vai ser do Brasil — funcionários que não atuem corretamente dentro das empresas serão funcionários que atuam contra a vontade da direção.

Por que eu dei esse exemplo? Porque, na realidade, nós não temos que pensar num Estado onipotente, que esteja em todos os lugares, com a Polícia Federal acessando *site* para ver se encontra algo. É importante que nós tenhamos o apoio da sociedade civil e das empresas em todos os crimes, inclusive cibernéticos.

Se o Google já faz essa verificação e descobre pornografia infantil, por que ele não ter essa obrigação, como tem nos Estados Unidos — não estou reinventando a roda —, de informar à Polícia Federal os crimes que estão sendo cometidos? Seria muito interessante, porque isso facilitaria o trabalho da Polícia e do Ministério Público nesses crimes.

Neste último, estou puxando bem a brasa para a minha sardinha. Em vários casos, isso é muito comum. E o Xvideos é um caso: a pessoa jurídica é sediada na Austrália, o *site* é sediado em Praga, e eles usam um provedor de acesso à Internet sediado na Suécia. Para onde se manda a cooperação internacional? Austrália, Suécia ou República Tcheca? Estamos em contato com a Xvideo exatamente verificando o cumprimento. Mas isso às vezes causa problemas. Já houve caso de cooperação que mandamos para a Suécia, que afirmou que não tinha como cumprir. Além disso, as empresas correm rápido.

Seria interessante que os provedores de serviço que atuassem no Brasil tivessem a obrigação — obrigação bem consumerista — de informar no *site* onde é sua sede, para efeito de cooperação internacional, porque, não sendo possível cumprir a ordem judicial brasileira, já saberíamos de antemão onde cumprir essa cooperação internacional.

Vou deixar minha apresentação, terminei falando um pouco rápido. Tentei ser bem didático em todas as questões. Estamos à disposição tanto para o debate posterior quanto para a discussão do projeto de lei, que, repito o que disse no começo, vem em muito boa hora. Foi um prazer estar aqui e discutir tema tão importante para a investigação brasileira.

Muito obrigado.



**A SRA. PRESIDENTA** (Deputada Laura Carneiro) - Agradeço ao Dr. Carlos Bruno Ferreira da Silva e ao Dr. Pablo Barcellos Bergmann, as contribuições.

A Relatora do projeto, é claro, de alguma maneira, vai tentar adequá-lo à nova realidade. Vamos fazer não uma audiência pública, mas uma mesa de debates e discutir os textos que saíram da CPI do Crime Cibernético. Não sei se os senhores acompanharam, mas são vários textos importantes que conseguimos votar, inclusive sobre bloqueio, para, de alguma maneira, vermos o que bate de um com outro, ou acabamos fazendo muitos projetos de lei.

A vantagem deste projeto de lei é que, aprovado, volta ao Senado. Se não se alterar nada, se simplesmente suprimirmos, já está aprovado e vai para sanção. Se alterarmos o texto, por isso a preocupação de alteração que implique qualquer outra modificação, a matéria volta ao Senado, mas, claro, já não mais como órgão revisor, mas como órgão principal. Aí vira lei também. Lá é sempre mais rápido do que aqui — a matéria vem daqui, vai para lá, volta para cá —, porque na Câmara dos Deputados são 513 Deputados. Então, no Senado Federal a velocidade para analisar matéria acaba sendo maior do que a nossa. Talvez as alterações nesse projeto sejam mais rápidas, para o benefício da legislação, do que as alterações feitas pela própria Câmara dos Deputados.

Peço desculpas aos senhores, porque hoje é um dia absolutamente complicado, quando provavelmente votaremos na CCJ matéria complicada da Receita Federal. Hoje é um dia atípico. Bom, depois que Trump ganhou a eleição, tudo é atípico. (*Riso.*) Enfim, há quem goste. Isso é o mais grave.

Agradeço a presença e a palestra aos senhores. Vamos manter contato. A contribuição foi enorme. No que pudermos construir juntos, agradeço.

Aproveito, portanto, para agradecer a todos que nos honraram não só com suas exposições e esclarecimentos, mas também com sua presença.

Antes de encerrarmos, relembro que amanhã, 10 de novembro, a Comissão fará uma visita, em missão oficial, a Rio Branco, Capital do Acre, em atendimento a requerimento do Deputado Rocha. Os Deputados serão recebidos pelas autoridades locais, entre elas o Secretário de Segurança Pública, o Diretor da Administração Penitenciária, o Comandante da Polícia Militar. Na programação consta o Encontro Regional da Assembleia Legislativa do Acre, quando discutiremos a situação da





Segurança Pública no Estado, especialmente os recentes ataques criminosos ocorridos na sua Capital, seguida de visita ao presídio de Rio Branco.

Nada mais havendo a tratar, vou encerrar os trabalhos. Antes, porém, convoco reunião de audiência pública para o dia 22 de novembro, terça-feira, às 11 horas, no Plenário 6, para debatermos com o Exmo. Sr. Ministro da Justiça a federalização da segurança pública do Distrito Federal, em atendimento ao Requerimento nº 170, de 2016, de autoria do Deputado Laerte Bessa.

Declaro encerrada a presente reunião.