Nota Técnica

Propostas para o Relatório Final da CPICIBER

(considerada a versão II, de 11/04/2016)

aos deputados relatores da Comissão Parlamentar
de Inquérito de Crimes Cibernéticos - CPICIBER.

Apresentação

Este documento visa oferecer, de forma detalhada, insumos ao Relatório Final da Comissão Parlamentar de Inquérito da Câmara dos Deputados sobre Crimes Cibernéticos - CPICIBER, considerados os termos da segunda versão, divulgada em 11 de abril de 2016. O objetivo é viabilizar o **combate aos cibercrimes** de maneira equilibrada com a **proteção de direitos fundamentais**.

O texto a seguir, elaborado com o propósito de refletir as preocupações diversas e plurais da sociedade civil, é resultado direto do trabalho conjunto das seguintes organizações: **Coding Rights, Instituto Beta: Internet e Democracia - IBIDEM, Intervozes – Coletivo Brasil de Comunicação Social** e **Artigo 19**.

Objetivamente, oferecemos a seguir **nove propostas** de mudanças, especialmente modificações e supressões nos novos projetos de lei, mas também alterações quanto às indicações e recomendações constantes do texto do relatório final.

Em cada proposta, devidamente numerada, indicamos inicialmente o trecho do relatório final ao qual ela se refere, seguido de um quadro resumo da sugestão de modificação e, por fim, as justificativas correspondentes, pormenorizadas conforme a complexidade das questões.

PROPOSTA Nº 1

SUBSTITUIR CONCEITOS ERRONEAMENTE DEFINIDOS OU IRRELEVANTES

PARTE II - Constatações e Conclusões
1 - Introdução
1.1.3 Conceitos importantes

Proposta nº 1

Remover os termos "mail bomb", "worm", "wikileaks", "quebra de senha", "denial of service", "sniffer", "backdoor", "deep web" e "botnets" e acrescentar os seguintes:

- **criptografia:** o estudo das técnicas de se comunicar de forma segura quando se tem alguém escutando o canal de comunicação. Através da criptografia e possível garantir a confidencialidade, a autenticidade e a integridade de mensagens e documentos.
- **criptografia ponta-a-ponta (*end-to-end*):** uma maneira de se criptografar mensagens ou arquivos para outras pessoas de forma que somente elas possam acessá-las; as *chaves* da criptografia ficam armazenadas nos dispositivos, de modo que o provedor de aplicação não pode vê-las.
- **backdoor:** trecho escondido de um programa que permite que quem o desenvolveu ganhe acesso ao computador que o executa ou possa quebrar a sua criptografia.
- **segurança cibernética:** assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (Estratégia de SIC, GSI/PR, atual Casa Militar).
- **deep web:** compreende todas as páginas web (ou seja, tudo que pode ser acessado pelo navegador) que não estão indexadas e catalogadas nos grandes mecanismos de busca, como Google, Bing e DuckDuckGo. O termo foi inicialmente cunhado para representar a grande parcela da web que não pode ser encontrada nestes portais, indicando que a web é muito maior do que parece à primeira vista – daí a metáfora comum da web "superficial" como a ponta de um iceberg. A *deep web* obedece ao mesmo ordenamento jurídico que a *surface web*; não há de fato distinção prática entre sites dentro e fora da *deep web* para um juiz ou agente.
- **pedofilia:** transtorno psiquiátrico em que um adulto ou adolescente mais velho sente uma atração sexual primária ou exclusiva por crianças pré-púberes, geralmente abaixo dos 11 anos de idade.
- **abuso sexual de menor:** forma de abuso infantil em que um adulto ou adolescente mais velho usa uma criança ou adolescente mais jovem para estimulação sexual, incluindo a participação em obras de exploração pornográfica infantil.
- **exploração pornográfica infantil:** forma ilegal de pornografia, em que participam crianças e adolescentes.

O Relatório Final, na Introdução da *Parte II - Constatações e Conclusões* (pág. 62), enumera conceitos considerados importantes "*quando se cuida de analisar a Internet e todas as circunstâncias a ela relacionadas*".

Todavia, em 8 páginas do documento, a lista declaradamente compilada "*sem a pretensão, obviamente, de exaurir o tema*", contempla definições escolhidas de forma arbitrária. Muitos dos termos não foram mencionados sequer uma vez nas audiências da CPICBER.

Uma pesquisa por termos, feita a partir das notas taquigráficas de todas as reuniões até o Seminário do dia 29 de março, permitiu elaborar a seguinte tabela, em que se comparam os termos sem definição e aqueles constantes da lista de conceitos do Relatório Final:

"Conceitos importantes" do relatório #CPICIBER			
Não estão definidos		Estão definidos	
termo	menções	termo	menções
cibernética / ciber-	1137	deface	3
criptografia / criptograf-	263	spyware	3
pedofilia	238	Wikileaks	3
privacidade	225	worm	1
anonimato / anonim-	156	hoax	0
pornografia infantil	152	mail bomb	0
segurança da informação	138	sniffer	0

PROPOSTA Nº 2

REDAÇÃO MAIS PRECISA AO ART. 154-A DO CÓDIGO PENAL

PARTE III - Proposições e Recomendações
1 - Projetos de Lei
1.2 – Projeto de Lei para alterar a redação do art. 154-a do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático

Proposta nº 2

Alterar a redação do Projeto de Lei proposto pelo Relatório, da seguinte maneira:

Art. 2º O artigo 154-A do Decreto-Lei no 2.848, de 7 de dezembro de 1940, passa a vigorar com a seguinte redação:

~~Invasão de~~ **Acesso indevido a** dispositivo informático

Art. 154-A. ~~Invadir~~ **Acessar** **indevidamente** dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou **com o fim de** instalar vulnerabilidades para obter vantagem ilícita:

O PL é escrito, justificado e mencionado nos seguintes trechos:

- Item 2.4.1 – "*Melhor tipificação do tipo penal de invasão de dispositivo informático contido na Lei Carolina Dieckmann (Lei nº 12.737/12)*" da sub-relatoria de Segurança Cibernética no Brasil, do deputado Rodrigo Martins (pág 131);
- Item nº 12 das Conclusões do Relator, deputado Espiridião Amin (pág. 160).
- Projeto de Lei nº 1.2 – "*altera a redação do art. 154-A do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático*" (pág. 174).

Quais condutas exatamente se buscam tipificar e que já não estejam previstas no atual art. 154-A do Código Penal (Decreto-Lei nº 2.848), que trata da finalidade de "*obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita*"?

O tipo penal atualmente em vigor, apesar de conter problemas, mostra-se mais equilibrado que a redação proposta, pois define a conduta de forma mais restrita, impedindo o enquadramento de condutas que não sejam o alvo específico da proteção jurídica em questão.

A alteração proposta pelo relator na segunda versão do projeto de lei, com vistas a superar as críticas de que a redação seria muito vaga, não resolve o problema. A expressão "*acesso indevido*", combinada ao restante do tipo penal proposto, mantém o caráter genérico, podendo abarcar uma variedade de condutas não necessariamente ilícitas ou prejudiciais. Por exemplo, legítimas investigações de segurança, que não ocorreriam em um ambiente de exigência de autorização, seriam criminalizadas no texto proposto pelo relator, mas não na nossa sugestão.

Consideramos especialmente vago o trecho "*expondo os dados informatizados a risco de divulgação ou de utilização indevidas"*. O termo "risco" torna inexigível haver efetiva divulgação ou a utilização indevida dos dados. Mas o quê exatamente caracteriza esse risco? Basta acessar ou armazenar os dados?

A ausência de uma definição para o significado de "risco" se agrava porque associada à expressão "*utilização indevida*". No limite, qualquer acesso a um sistema informatizado ou a dispositivo informático pode expor os dados a risco de "*divulgação ou de utilização indevidas*".

O dolo e o real risco de dano se demonstram mais concreta e adequadamente na delimitação de que o crime ocorre quando o acesso ocorre "*sem a autorização expressa ou tácita do titular do dispositivo*". A menção ao titular é um elemento do tipo fundamental, presente também na expressão vigente "*dispositivo informático alheio*".

Um dos postulados ínsitos ao princípio da legalidade no direito penal é o princípio da taxatividade (*lex certa*), segundo o qual o tipo penal deve ser claro, preciso e determinado, permitindo ao cidadão a real consciência acerca da conduta punível criminalmente pelo Estado.

Defendemos a manutenção da maior parte do art. 154-A atualmente vigente. Concordamos, porém, que se substitua "invadir" por "*acessar indevidamente*", termo mais adequado do ponto de vista da redação técnico-jurídica, pois não se trata de coibir a *invasão,* tomada como a entrada presencial de alguém em algum lugar, mas apenas de vedar um acesso virtual a dados.

Ressalte-se, como já dito, que esse termo ficará vago e impreciso se não vier acompanhado de todas as delimitações atualmente presentes no texto do Código Penal.

PROPOSTA Nº 3

SUBSTITUIR UTILIZAÇÃO DO FISTEL PELA UTILIZAÇÃO DO FNSP

PARTE III - Proposições e Recomendações
1 - Projetos de Lei
1.3 – Projeto de Lei visando à alteração da Lei nº 5.070, de 7 de julho de 1966, para autorizar o uso dos recursos do Fistel por órgãos da polícia judiciária

Proposta nº 3

Não alterar o art. 5º da Lei nº 5.070/1966, que trata do FISTEL – Fundo de Fiscalização das Telecomunicações, mas sim o art. 4º da Lei nº 10.201/2001, que regula o FNSP – Fundo Nacional de Segurança Pública, nos seguintes termos:

Art. 2º O artigo 4º da Lei nº 10.201, de 14 de fevereiro de 2001, passa a vigorar acrescido do seguinte parágrafo:

"Art. 4º .....

.....

§ 9º. Até 10 % (dez por cento) das transferências para o Tesouro Nacional poderão ser utilizados pelos órgãos da polícia judiciária de que trata o artigo 4o da Lei nº 12.735, de 30 de novembro de 2012." (NR)

Art. 3º Esta lei entra em vigor um ano após sua publicação oficial.

A proposta de PL a ser alterada é escrita, justificada e mencionada nos seguintes trechos do relatório final:

- Item 2.4.4 – "*Alocação de recursos do Fistel – Fundo de Fiscalização das Telecomunicações – para manutenção das polícias especializadas*" da sub-relatoria de Segurança Cibernética no Brasil, do deputado Rodrigo Martins (pág 134).
- Item nº 14 das Conclusões do Relator, deputado Espiridião Amin (pág 164).
- Projeto de Lei nº 1.3 – "visando à alteração da Lei n o 5.070, de 7 de julho de 1966, para autorizar o uso dos recursos do Fistel por órgãos da polícia judiciária" (pág 178).

Sem dúvida, o Estado precisa se aprimorar para combater de forma específica os cibercrimes. Entretanto, esse objetivo não pode ser alcançado mediante um desvio de finalidade do FISTEL - Fundo de Fiscalização das Telecomunicações.

Especialmente quando existe o **Fundo Nacional de Segurança Pública - FNSP** (criado pela Lei nº 10.201/2001), com previsão legal específica para esse propósito, com a expressa exigência de compromisso com resultados, enumeração de órgãos que podem ter acesso aos recursos, definição de prazo de realização, e disciplina de forma e condições de aplicação:

> ***Art. 1º*** *Fica instituído, no âmbito do Ministério da Justiça, o Fundo Nacional de Segurança Pública – FNSP, com o objetivo de apoiar projetos na área de segurança pública e de prevenção à violência, enquadrados nas diretrizes do plano de segurança pública do Governo Federal. (Redação dada pela Lei nº 10.746, de 10.10.2003)*
> *(...)*
>
> ***Art. 4º*** *O FNSP apoiará projetos na área de segurança pública destinados, dentre outros, a: (Redação dada pela Lei nº 10.746, de 10.10.2003)*
> ***I*** *- reequipamento, treinamento e qualificação das polícias civis e militares, corpos de bombeiros militares e guardas municipais; (Redação dada pela Lei nº 10.746, de 10.10.2003)*
> ***II*** *- sistemas de informações, de inteligência e investigação, bem como de estatísticas policiais; (Redação dada pela Lei nº 10.746, de 10.10.2003)*
> ***III*** *- estruturação e modernização da polícia técnica e científica; (Redação dada pela Lei nº 10.746, de 10.10.2003)*
> *(...)*
> ***V*** *- programas de prevenção ao delito e à violência. (Redação dada pela Lei nº 10.746, de 10.10.2003)*

Por sua vez, os recursos do FISTEL, disciplinados pela Lei nº 5.070/1966 (com redação dada pela Lei nº 9.472/1997), têm previsão clara de aplicação exclusiva para a fiscalização de serviços de telecomunicações.

> ***Art. 1º****. Fica criado um fundo de natureza contábil, denominado "Fundo de Fiscalização das Telecomunicações", destinado a prover recursos para cobrir despesas feitas pelo Governo Federal na execução da fiscalização de serviços de telecomunicações, desenvolver os meios e aperfeiçoar a técnica necessária a essa execução.*
>
> ***Art. 3°*** *Além das transferências para o Tesouro Nacional e para o fundo de universalização das telecomunicações, os recursos do Fundo de Fiscalização das Telecomunicações - FISTEL serão aplicados pela Agência Nacional de Telecomunicações exclusivamente:* (Redação dada pela Lei nº 9.472, de 1997)
> ***a)*** *na instalação, custeio, manutenção e aperfeiçoamento da fiscalização dos serviços de telecomunicações existentes no País;*
> ***b)*** *na aquisição de material especializado necessário aos serviços de fiscalização;*
> ***c)*** *na fiscalização da elaboração e execução de planos e projetos referentes às telecomunicações;*

> ***d)*** *no atendimento de outras despesas correntes e de capital por ela realizadas no exercício de sua competência.* (Incluído pela Lei nº 9.472, de 1997)

Em primeiro lugar, mostra-se necessário esclarecer que conexão à Internet não é propriamente um serviço de telecomunicação, mas sim um **serviço de valor adicionado**, conforme definição vigente da Norma 04/1995 do Ministério das Comunicações <http://www.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148>, que regulamenta de forma específica "*o uso de meios da Rede Pública de Telecomunicações para o provimento e utilização de Serviços de Conexão à Internet*". Por essa norma, a conexão à Internet é considerada juridicamente como um serviço que acrescenta a uma rede de telecomunicações preexistente os meios ou recursos que criam novas utilidades específicas, ou novas atividades produtivas, relacionadas com o acesso, armazenamento, movimentação e recuperação de informações.

Logo, o acesso a um serviço *online* é só um uso particular de um serviço de telecomunicação (telefonia fixa, móvel, TV por assinatura, redes de banda larga), mas não se confunde com ele. Portanto, não pode ser alvo de fiscalização apoiada em investimentos de recursos do FISTEL, o qual, repita-se, destina-se exclusivamente à fiscalização de serviços de telecomunicações.

Há tantos problemas na atuação das operadoras de telecomunicações, as quais sempre estão no topo das listas de reclamações dos consumidores, que não faz sentido redirecionar para outros propósitos os recursos de um fundo destinado a fiscalizar esses serviços e, por esse meio, contribuir ao aprimoramento de sua qualidade. Em especial quando os constantes contingenciamentos do fundo prejudicam a própria Anatel no exercício de sua função, como alerta a recomendação do Ministério Público Federal feita à Presidência da República e a Ministérios ao final de 2014 <http://noticias.pgr.mpf.mp.br/noticias/noticias-do-site/copy_of_consumidor-e-ordem-economica/mpf-recomenda-correta-aplicacao-dos-recursos-devidos-a-anatel-em-defesa-dos-consumidores-nas-telecomunicacoes>.

A utilização do FISTEL por órgãos da polícia judiciária agravaria esses problemas, por insistir na alocação dos recursos em finalidade estranha aos objetivos do fundo, que já não vêm sendo cumpridos a contento. Ainda mais grave, a proposta do relatório da CPICIBER redireciona seus fundos para a vigilância dos usuários de Internet, majoritariamente ocupados em atividades lícitas e que, repita-se, não se enquadram sequer como serviço de telecomunicação.

Nesse cenário, não se justifica o uso de parte do FISTEL para equipar a polícia no combate a crimes cibernéticos, por meio de uma falaciosa "fiscalização" dos usuários. Não há problema em equipar mais e melhor a polícia, mas os recursos devem vir de fontes adequadas, já existentes, como o citado FNSP, sem prejudicar outras finalidades.

Logo, mesmo diante da possibilidade de usos ilegais da Internet, os maiores investimentos nesse momento devem estar voltados ao fomento do uso da rede, a partir de sua finalidade social. Investimentos em banda larga podem contribuir e muito para a qualidade dos serviços de telecomunicações e de valor adicionado. Também por isso o governo federal vem trabalhando com a possibilidade de aplicar o FISTEL no financiamento de suas políticas de acesso à banda larga, o que novamente não pode ser desprezado na análise desse projeto de lei. Como disse Tim Berners-Lee, inventor da Web, em sua Carta Aberta aos Legisladores Brasileiros:

"Sugestões de que o dinheiro destinado a conectar mais brasileiros seja realocado para fundos de policiamento da rede são iniciativas difíceis de se entender, ainda mais quando quase metade do país ainda não pode se beneficiar de um acesso à Internet com frequência".

PROPOSTA Nº 4

REGRAS PARA INDISPONIBILIZAÇÃO DE CONTEÚDO INFRINGENTE IDÊNTICO

PARTE III - Proposições e Recomendações
1 - Projetos de Lei
1.5 – Projeto de Lei determinando a indisponibilidade de cópia de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e dá outras providências

Proposta nº 4

Alterar a redação do Projeto de Lei proposto pelo Relatório, da seguinte maneira:

Art. 1º Esta Lei modifica o Marco Civil da Internet, Lei n o 12.965, de 23 de abril de 2014, determinando a indisponibilidade de cópia de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e dá outras providências.

Art. 2º A Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, passa a vigorar acrescida dos seguintes dispositivos:

Art. 19-A Quando se tratar ~~Os provedores aplicação deverão tomar as providências técnicas, tendo em conta o conjunto~~ de cópia de ~~meios suscetíveis~~ conteúdo infringente que já tenha sido objeto de ordem judicial determinando sua indisponibilização, o provedor de ~~serem razoavelmente utilizados~~ aplicação, no âmbito e nos limites técnicos de ~~suas aplicações, para assegurar~~ seu serviço, de forma diligente, deverá torná-la indisponível sempre que ~~o conteúdo infringente, objeto da ordem judicial ou da~~ houver nova notificação ~~de~~ que ~~trata esta Seção, continue indisponível em caso de cópia, dispensada~~ aponte a ~~necessidade de nova ordem~~ localização inequívoca da cópia e a decisão judicial ~~ou notificação para~~ que fundamenta a ~~retirada desses novos materiais.~~ sua indisponibilização.

Parágrafo único. Para os efeitos deste artigo, é considerada cópia o conteúdo idêntico ao original ~~ou que contenha parte majoritária do conteúdo original~~ e que continue a configurar a característica considerada como infringente;

Íntegra da nossa proposta de um novo Art. 19, sem marcações de mudanças:

Art. 19-A Quando se tratar de cópia de conteúdo infringente que já tenha sido objeto de ordem judicial determinando sua

> indisponibilização, o provedor de aplicação, no âmbito e nos limites técnicos de seu serviço, de forma diligente, deverá torná-la indisponível sempre que houver nova notificação que aponte a localização inequívoca da cópia e a decisão judicial que fundamenta a sua indisponibilização.
>
> **Parágrafo único.** Para os efeitos deste artigo, é considerada cópia o conteúdo idêntico ao original que continue a configurar a característica considerada como infringente;

A proposta de PL a ser alterada é escrita, justificada e mencionada nos seguintes trechos:

- Item 2.3.1 – "*Retirada de conteúdos infringentes repetidos*" da sub-relatoria de Crimes Contra a Honra e Outras Injúrias, do deputado Daniel Coelho (pág 127)
- Item nº 8 das Conclusões do Relator, deputado Espiridião Amin (pág 161).
- Projeto de Lei nº 1.7 – "*altera o Marco Civil da Internet, Lei n o 12.965, de 23 de abril de 2014, determinando a indisponibilidade de cópia de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e dá outras providências*" (pág 185).

Concordamos que não faz sentido exigir novas ordens judiciais e, portanto, a proposição de novas ações, a fim de que se indisponibilizem conteúdos já considerados infringentes pelo Poder Judiciário. Tratando-se de cópia de conteúdo já submetido ao crivo judicial e considerado ilícito, a indisponibilização pode se dar por meio de mera notificação do interessado, desde que a notificação permita a localização inequívoca do material (conforme exigência do art. 19, §1º, do Marco Civil da Internet - Lei nº 12.965/2014) e aponte a decisão que o reputou infringente.

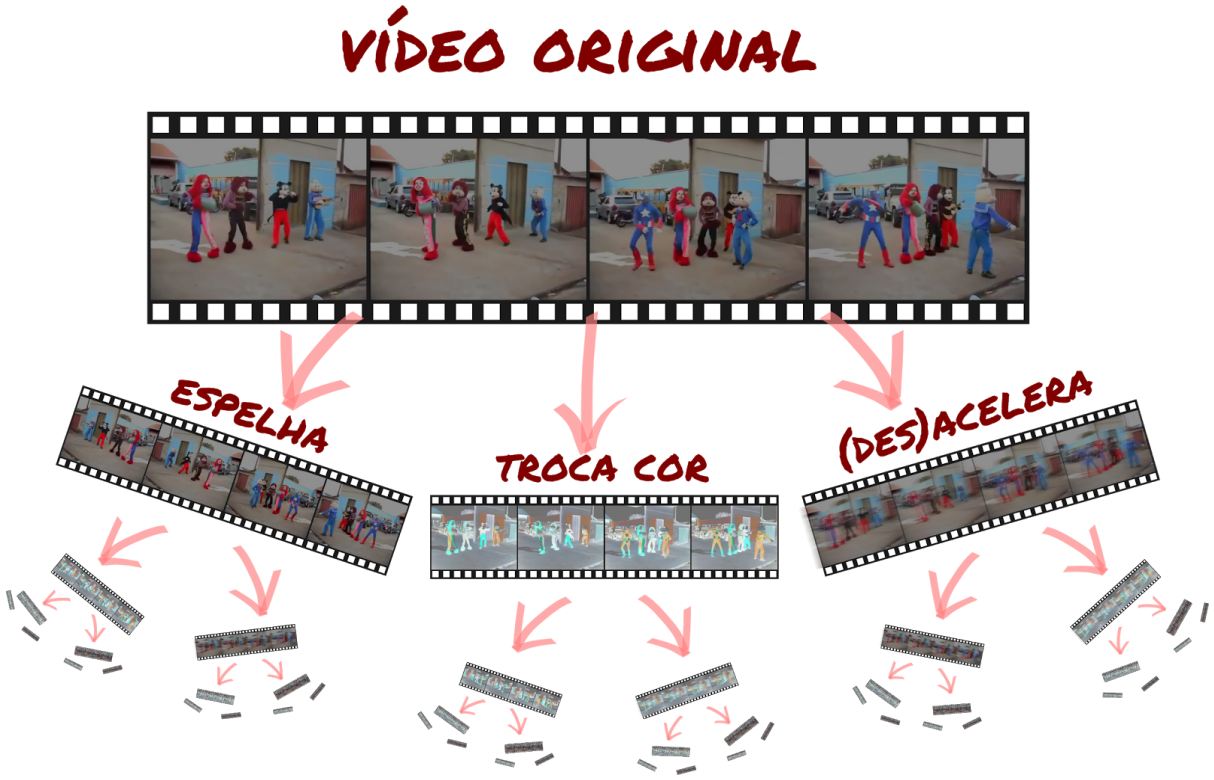
As hipóteses de responsabilização dos provedores de aplicações por descumprimento de mera notificação são excepcionais no Marco Civil da Internet. O objetivo dessa norma é equilibrar a garantia da liberdade de expressão e do acesso à informação com a proteção de outros direitos no ambiente *online*, entre eles a honra, a imagem, o nome etc.. A figura institucional competente para avaliar tal equilíbrio é o juiz, cuja imparcialidade e o saber jurídico são necessários para decidir o conflito de interesses nas controvérsias sobre indisponibilização de conteúdo online.

Esse papel não pode ser conferido ao provedor de aplicações, que em geral tenderá a seguir, por interesses econômicos, o caminho da segurança jurídica, retirando sempre os conteúdos, como forma de evitar processos judiciais e o pagamento de indenizações. Essa via abriria larga margem para a censura online. Por sua vez, a regra geral do Marco Civil é a responsabilização dos provedores de aplicações pelos conteúdos de terceiros apenas se aqueles intermediários descumprem ordem judicial que determinou a indisponibilização. Entretanto, a sugestão posta no relatório final insere no Marco Civil nova hipótese de notificação e retirada ("notice and takedown"), em lógica incompatível com a regra geral.

Cria, portanto, uma antinomia, por não observar a norma do § 1º do art. 19, que exige, para validade da ordem judicial, a "*identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material*".

Além disso, a proposta do relatório, ao criar uma dinâmica de constante monitoramento dos conteúdos pelo provedor de aplicações, se mostra perigosa e complexa. Sendo possível desenvolver ferramentas automáticas de identificação de conteúdo, a medida poderia parecer de exigência razoável em relação às grandes aplicações online, como Facebook. Mas a maior parte dos sites e aplicativos, por sua estrutura reduzida, teria grande dificuldade para investir na operação de ferramentas desse tipo. A obrigatoriedade significaria uma relevante barreira à entrada, impactando negativamente na inovação na rede.

No entanto, as dificuldades não param aqui e podem atingir mesmo as grandes empresas. Conforme Pedro Markun, em audiência realizada por esta CPI, na identificação de "conteúdos repetidos", é comum que vídeos bloqueados sejam relançados na rede com pequenas alterações como espelhar a imagem (*flipar*, como diz Markun), mudar a velocidade de reprodução ou mudar sutilmente as cores da imagem. Com a combinação de algumas destas modificações já é possível produzir exponencialmente variantes que são, no mínimo, um grande desafio para técnicas de identificação de conteúdo repetido como PhotoDNA e *hashing*, mencionadas na CPI. Mesmo que a aplicação disponha desses mecanismos de identificação, técnicas como as mencionadas acima podem fazer com que o mecanismo falhe nessa identificação e o provedor de aplicações seja responsabilizado sem que tenha havido de fato dolo, ou mesmo culpa, na manutenção de conteúdo já considerado infringente.



Por isso, apresentamos como sugestão a solução de indisponibilizar a cópia de conteúdo mediante mera notificação. Com isso, não queremos que o ônus de "procurar o conteúdo" passe à vítima, mas acreditamos que o usuário afetado, melhor do que qualquer outro agente, terá conhecimento dos links que o ofendem e poderá reportá-los sem grande burocracia ao provedor de aplicações, que deverá indisponibilizá-los o mais rápido possivel, no âmbito e nos limites técnicos de seu serviço, sem necessidade de ordem judicial. Do contrário, estaríamos colocando os sites e aplicativos na posição de eternos vigias de conteúdo na Internet, o que causaria sérios impactos à sua atividade e mesmo aos usuários de forma geral, mais monitorados em relação às suas postagens. Nossa proposta visa compatibilizar a preocupação do relator à proteção da livre iniciativa, da livre concorrência, da liberdade de expressão e do acesso à informação. Por fim, justificamos outros três pontos que merecem atenção:

1. Considerando a redação proposta e o objeto mais amplo, atinente à responsabilização civil, após ordem judicial específica, por danos decorrentes de conteúdo gerado por terceiros, mostra-se mais adequado o novo artigo ser numerado como 19-A e não 21-A.

2. Buscando precisão terminológica, a proposta ora apresentada se exclusivamente do termo "indisponibilização", sem fazer referência ao termo "retirada". Tanto do ponto de vista teórico jurídico, quanto pela perspectiva prática tecnológica, "*retirar um conteúdo*" da Internet não é o mesmo que "tornar indisponível o acesso". O Marco Civil da Internet já se refere à "indisponibilização de conteúdo", reforçando ser essa a terminologia adequada.

3. Na definição de cópia mantemos apenas os casos de "cópia idêntica", isso porque a expressão "parte majoritária" é um termo vago, que replicaria no texto do Marco Civil um dos grandes problemas na legislação de direito autoral, que considera legal a utilização pessoal de "pequenos trechos" de obras intelectuais (art. 46, II, da Lei nº 9.610/1998) e até hoje se demonstra como baliza de controversa aplicação prática. Não é incomum que conteúdos na Internet sejam parcialmente replicados com sentidos diferentes, sem que nesse novo contexto sejam considerados ofensivos. Pequenas alterações podem levar a isso e, novamente, não deve caber ao provedor de aplicações decidir se, após a alteração, o conteúdo continua infringente ou não.

PROPOSTA Nº 5

NÃO PERMITIR O ACESSO AO ENDEREÇO IP SEM ORDEM JUDICIAL

PARTE III - Proposições e Recomendações
1 - Projetos de Lei
1.2 – Projeto de Lei para alterar a redação do art. 154-a do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático

Proposta Nº 5

Remover Projeto de Lei que "*permite que a autoridade de investigação requisite, independentemente de autorização judicial, o endereço IP utilizado para a geração de conteúdo específico objeto de investigação criminal, mantidos por provedor de conexão ou de aplicação de internet*".

O PL é justificado e mencionado nos seguintes trechos:

- Item 2.3.2 – "Acesso ao endereço IP utilizado para a geração de conteúdo específico objeto de investigação criminal" da sub-relatoria de Crimes Contra a Honra e Outras Injúrias, do deputado Daniel Coelho (pág. 128).
- Item nº 11 das Conclusões do Relator, deputado Espiridião Amin (pág. 164).
- Projeto de Lei nº 1.6 – "permitindo que a autoridade de investigação requisite, independentemente de autorização judicial, endereço IP que identifique conteúdo ou serviço específico, objeto de investigação criminal, mantidos por provedor de conexão ou de aplicação de Internet" (pág. 190).

Primeiramente, a parte final do *caput* do art. 1º incorre em um erro conceitual, ao considerar a possibilidade de um "provedor de conexão" manter um conteúdo específico objeto de investigação criminal. Talvez a redação estivesse direcionada a permitir que a requisição pudesse ser feita a esse provedor, mas o texto proposto não alcança essa suposta finalidade.

Não obstante, em um contexto no qual o conteúdo investigado seja conhecido, permitir que a autoridade de investigação requisite, independentemente de autorização judicial, o endereço IP utilizado equivale a requisitar o próprio registro de acesso a aplicações, cuja disponibilização deve ser sempre precedida de autorização judicial, conforme os arts. 10, § 1º, 15, § 3º, 22 e 23 do Marco Civil da Internet. Mesmo que se trate apenas do endereço IP, desconectado de um conteúdo, esse dado será enquadrado como registro de conexão, conferindo-se a ele as mesmas garantias (arts. 10, §1º, 13, §5º, 22 e 23 do Marco Civil da Internet).

A permissão de qualquer acesso a dados pessoais de cidadãos sem ordem judicial não tem paralelo em legislações de países democráticos, os quais somente assim são considerados na medida em que respeitem precisamente as garantias fundamentais que estruturam um Estado de Direito. Direitos humanos não podem ser fragilizados a pretexto de atender à celeridade de uma investigação, por um procedimento que, na prática, pode significar uma porta aberta a arbitrariedades e a violações de direitos. Destaque-se que a previsão de eventual punição para o mau uso de dados pessoais não tem o condão de reparar o prejuízo decorrente da ofensa a uma garantia constitucional, notadamente se realizada de forma sistemática e em massa.

E embora a Polícia Civil seja menos conhecida do que a Polícia Militar por abusos e corrupção, a instituição conta com seus próprios escândalos: há poucos meses o inspetor-chefe da Corregedoria da Polícia Civil foi afastado do cargo por envolvimento "em acusações de favorecimento e tráfico de influência", acusações que enfrenta junto a seis corregedores,

segundo matéria da Agência Brasil <http://agenciabrasil.ebc.com.br/geral/noticia/2015-12/apos-denuncias-de-corrupcao-corregedor-da-policia-civil-de-sp-e-afastado>. Um vídeo em matéria do Estadão mostra dois policiais civis fugindo de promotores que iriam prendê-los no DEIC/SP sob acusação de receber propina em troca de vista grossa; é possível que a própria corregedoria, convocada pelos promotores para acompanhá-los, tenha avisado os policiais <http://sao-paulo.estadao.com.br/noticias/geral,corregedoria-da-policia-e-acusada-de-cobrar-mensalao-para-ajudar-corruptos,1814038>.

De acordo com dados da Ouvidoria de Polícia de São Paulo, entre 1998 e 2014 houve 591 delegados investigados a partir de denúncias na Ouvidoria, que resultaram em 144 punições; houve também 10 investigações contra "agentes de telecomunicações", com 4 policiais punidos. Sem desmerecer o importante trabalho de agentes policiais honestos, conceder acesso a dados sem ordem judicial, como o endereço IP no caso do Projeto de Lei sendo proposto, irá fatalmente gerar abusos.

Em resumo, a proposta cria uma antinomia, em burla à garantia, expressa no Marco Civil, de que depende sempre de ordem judicial a disponibilização dos registros de conexão e dos registros de acesso a aplicações de Internet. Trata-se de um direito específico que dá conteúdo ao devido processo legal, alcançado mediante um consenso legislativo, resultado de um amplo debate que culminou na Lei nº 12.965/2014, cuja importância democrática e precisão técnica não deveria ser desprezada pela CPI.

PROPOSTA Nº 6

NÃO PERMITIR O BLOQUEIO DE APLICAÇÕES

PARTE III - Proposições e Recomendações
1 - Projetos de Lei
1.7 – Projeto de Lei que possibilita o bloqueio de aplicações de Internet por ordem judicial

Proposta Nº 6

Retirar a proposta de que os provedores de conexão sejam colocados na posição de monitoramento de aplicações.

O PL em questão é escrito, justificado e mencionado nos seguintes trechos:

- Item 2.1.4 – "Violação de direitos autorais na internet" da sub-relatoria de Instituições Financeiras e Comércio Virtual, do deputado Sandro Alex (pág 121).
- Item 2.2.3 – Previsão de bloqueio, por meio de decisão judicial, dos sites que disponibilizam conteúdos ilícitos" da sub-relatoria de Crimes contra a Criança e o Adolescente do deputado Rafael Motta (pág 142).
- Item nº 7 das Conclusões do Relator, deputado Espiridião Amin (pág 160).
- Projeto de Lei nº 1.7 – "Possibilita o bloqueio de aplicações de internet por ordem judicial" (pág 196).

O bloqueio de páginas da Internet com a justificativa de proteção a direitos autorais é uma restrição desproporcional à liberdade de expressão, devido aos riscos associados de excesso de bloqueio e à falta geral de eficácia dessa medida. Mesmo em relação aos direitos de crianças e adolescentes o problema permanece, contrapondo esses dois riscos - o excesso de bloqueio, por um lado, e a eficácia duvidosa, por outro.

Embora o bloqueio de páginas da Internet seja colocado como último recurso a ser adotado, é muito claro que o expediente será usado de maneira abusiva e desproporcional tendo em vista, por exemplo, recentes decisões de bloqueio do aplicativo Whatsapp, que levou à detenção do vice-presidente para a América Latina do Facebook.

O juiz poderá determinar o bloqueio da aplicação inteira, deixando fora do ar um grande conjunto de conteúdos lícitos e legítimos, podendo, inclusive, prejudicar a comunicação dos usuários da rede de forma geral, como ocorreu com o Whatsapp ou poderia ocorrer se o Gmail ou Yahoo fossem bloqueados, por exemplo.

Ainda, embora a proposta tenha surgido mais especificamente de preocupações relacionadas com direitos autorais e direitos de crianças e adolescentes, a autorização inserida no art. 9º do Marco Civil da Internet é genérica o suficiente para abarcar quaisquer outras hipóteses que envolvam uma conduta criminosa e que o site ou aplicativo não estejam cumprindo a ordem judicial.

É certo que as aplicações devem respeitar as determinações do Judicário e as legislações processuais, cível e penal, já contêm instrumentos suficientes para dar efetividade à atividade jurisdicional. Prever essa autorização geral de bloqueio de aplicações no Marco Civil da Internet dá mais margem a abusos do que, de fato, resolve o problema que se quer atacar.

Em relação a conteúdo ofensivo, por exemplo, é notória a ineficiência da medida, uma vez que bloqueada uma página, surgem outras inúmeras exatamente com o mesmo conteúdo dada a natureza da rede. Sem mencionar que muitos conteúdos protegidos por direitos autorais não são compartilhados em uma plataforma específica, mas parcialmente compartilhados entre pares. Ainda pior, ordens de bloqueio para impedir futuras violações de direitos são uma forma de censura prévia.

Por fim, o bloqueio de sites fere a neutralidade de rede, um dos principais direitos garantidos pelo Marco Civil da Internet. A fim de cumprir a ordem judicial, provedores de conexão a internet serão obrigados a vasculhar os pacotes de dados com o objetivo de encontrar o conteúdo infrigente ou impedir o acesso a ele. É um precedente bastante perigoso que pode ensejar que a técnica seja usada com fins comerciais e outros interesses.

PROPOSTA Nº 7

NÃO AMPLIAR O ACESSO AO CADASTRO DE USUÁRIOS DE TELEFONES PRÉ-PAGOS

PARTE III - Proposições e Recomendações
2 – Propostas de Fiscalização e Controle
2.1 – Propõe que a Comissão de Ciência e Tecnologia, Comunicação e Informática, fiscalize, com auxílio do Tribunal de Contas da União – TCU, as ações de acompanhamento e controle da Agência Nacional de Telecomunicações – ANATEL acerca da correta implementação e utilização dos cadastros de usuários de telefones pré-pagos

Proposta nº 7

Remover proposta de fiscalização do controle da ANATEL sobre cadastros de usuários de telefones pré-pagos.

A proposta é mencionada nos seguintes trechos:

- Item 2.4.5 – "Fiscalização por parte do TCU das ações da Anatel no que diz respeito ao cadastro dos acessos pré-pagos à internet" da sub-relatoria de Segurança Cibernética no Brasil, do deputado Rodrigo Martins (pág. 135).
- Item nº 15 das Conclusões do Relator, deputado Espiridião Amin (pág. 164).
- Proposta de fiscalização e controle nº 2.1 – "propõe que a Comissão de Ciência e Tecnologia, Comunicação e Informática, fiscalize, com auxílio do Tribunal de Contas da União – TCU, as ações de acompanhamento e controle da Agência Nacional de Telecomunicações – ANATEL acerca da correta implementação e utilização dos cadastros de usuários de telefones pré-pagos" (pág 199).

A mera existência de um cadastro de usuários de telefone pré-pago é problemática. Incluir novos atores públicos na gestão desse banco de dados fragiliza a privacidade e a liberdade de expressão, sem que se conheça publicamente indícios empíricos quaisquer de que a atividade polícia tenha tido sucesso no combate ao crime mediante tal ferramenta.

Vale aduzir que o art. 5º, XII, da Constituição Federal veda o anonimato no âmbito da "*liberdade de manifestação do pensamento*". Assim, (i) o anonimato é vedado apenas para se expressar, mas não para acessar informação, o que corresponde a "ir e vir" nas redes; e (ii) a proibição ao anonimato deve ser flexibilizada quando se verificar que se trata de uma condição necessária à própria manifestação individual, o que pode ocorrer mesmo em um contexto democrático, por exemplo, nos mecanismos de denúncia anônima e no e sigilo de fonte jornalística.

O anonimato não se confunde, por si só, com a efetiva prática de um crime. Sugerimos expressamente a reinterpretação e proteção do anonimato como forma de exercício do direito

humano de acesso à informação, virtual ou presencial, mas também como mecanismo de segurança para opiniões e expressão de ideias contra eventuais ataques arbitrários e ilegais.

Por sua vez, a privacidade deve ser entendida como o direito que cada pessoa tem de traçar, sobre a sua própria vida, a linha que separa a porção compartilhada e a parte reservada. Ela constitui uma escolha livre e individual, de acordo com suas próprias convicções e forma de ver o mundo. Uma garantia de que é possível ter uma vida privada. Nesse conceito amplo, a privacidade vai muito além do ditado "quem não deve não teve". Não se trata de um temor contra a revelação de segredos, de um medo de que aspectos obscuros sejam conhecidos. Pensar assim levaria à conclusão de que seria necessário ter feito algo errado para ter direito à privacidade, um contrassenso cruel no qual justamente as pessoas que se portam corretamente seriam punidas com a redução da proteção sobre a própria vida.

A privacidade não é uma defesa para criminosos, nem uma cobertura para condutas erradas. É uma garantia de liberdade, para preservar a individualidade das pessoas, nos termos em que elas mesmas quiserem. Do conforto do lar ao ambiente de trabalho, passando pelo uso de um celular pré-pago, o que importa é ter a opção sobre abrir ou fechar porta do quarto, sobre revelar ou não o valor do seu contracheque, sobre vincular ou não o CPF a um número de telefone, sem nenhuma imposição, e com a segurança de que não haverá desrespeito.

Consideradas a ressignificação da vedação ao anonimato, e firme na defesa da privacidade, é necessário concluir que se a legislação em vigor exige que a ANATEL mantenha um cadastro de usuários de telefones pré-pagos, o risco de vazamento de dados ou acesso abusivo apenas aumenta caso se submeta esse banco de dados ao escrutínio da Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados, com auxílio do Tribunal de Contas da União.

Sem desmerecer os nobres propósitos da proposta, tampouco ignorando a lisura e seriedade das instituições legislativas, o fato é que a própria comunicação desses dados entre diversas pessoas permitiria incontáveis portas inadequadas de acesso ao cadastro, com consequências graves de dimensões incalculáveis para milhões de inocentes, que nem mesmo poderiam se proteger adequadamente contra qualquer incidente.

PROPOSTA Nº 8

NÃO INDICAR À ANATEL A ADOÇÃO DO IPV6

PARTE III - Proposições e Recomendações
3 – Indicações
3.5 – Indicação à Agência Nacional de Telecomunicações, sugerindo a adoção das medidas necessárias para a implantação do IPv6 no país

Proposta nº 8

Remover Indicação à Anatel para a implantação do IPv6, ou de tecnologia similar.

A indicação é mencionada nos seguintes trechos:

- Item 2.4.2 – "Guarda dos registros de conexão por todos os provedores de internet e migração para o IPv6 ou tecnologia similar" da sub-relatoria de Segurança Cibernética no Brasil, do deputado Rodrigo Martins. (pág 137);
- Item b) na seção "3 – Proposições Legislativas em Tramitação na Câmara cuja discussão se mostra importante";
- Item nº 13 das Conclusões do Relator, deputado Espiridião Amin (pág 163).
- Sub-item ii) do item nº 22 das Conclusões do Relator, deputado Espiridião Amin (pág 168).
- Item b) da seção "5 – Recomendações e Encaminhamentos da Comissão"

Não se sustenta a recomendação, direcionada à ANATEL - Agência Nacional de Telecomunicações, de que o IPv6 seja adotado como instrumento para identificar pessoas mais facilmente, a partir dos registros de conexão à Internet e registros de uso de aplicação *online*.

Primeiro porque a ANATEL, como reguladora de serviços de telecomunicações, nem sequer ostenta competência administrativa sobre o tema. Repita-se que a conexão à Internet não é propriamente um serviço de telecomunicação, mas um **serviço de valor adicionado**, conforme definição vigente da Norma 04/1995 do Ministério das Comunicações <http://www.anatel.gov.br/legislacao/normas-do-mc/78-portaria-148>. Portanto, não caberia à ANATEL essa atribuição de acelerar a implementação do IPV6.

Segundo, sabe-se que a retenção de dados indiscriminada viola direitos fundamentais como a privacidade e a liberdade de expressão, conforme defendido por diversos representantes da academia e da sociedade civil presentes nesta CPI, bem como pela Corte Interamericana de Direitos Humanos, pela Corte de Justiça Europeia e por Relatores Especiais da ONU. Não há estatísticas ou estudos que justifiquem esse caminho, mas apenas ilações anedóticas nas falas de delegados e outros representantes de setores policiais ou investigativos.

Terceiro, há um problema prático na adoção do IPv6 como meio de identificação de usuários. O Relatório Final pressupõe que o novo sistema permitiria superar a dificuldade do atual IPV4 em atribuir um endereço IP a um determinado dispositivo:

> *Esse problema decorre, na verdade, da escassez na quantidade de IPs disponíveis em sua versão 4, o qual seria solucionado com a adoção da versão 6, o chamado IPv6.*

No entanto, a proposta do relatório aparentemente não considerou que o sistema IPv6 conta, por padrão, com "**extensões de privacidade**" (*privacy extensions)*, presentes em quase todos os sistemas operacionais, que **geram continuamente endereços IP efêmeros e impedem o provedor de associá-los ao titular da conexão à Internet**.

São esses os três motivos principais que nos fazem recomendar que seja removida do relatório a indicação proposta quanto ao IPV6.

PROPOSTA Nº 9

NÃO ENDOSSAR A AMPLIAÇÃO DA GUARDA DE REGISTROS DE CONEXÃO

PARTE III - Proposições e Recomendações
5 – Recomendações e Encaminhamentos da Comissão
b) Guarda dos registros de conexão por todos os provedores de Internet

Proposta nº 9

Remover a promoção do PL 3237/15, que amplia o conceito de "administrador de sistema autônomo" para *aumentar* o alcance da retenção de registros de conexão à Internet.

O Projeto de Lei nº 3237/15, de autoria do Deputado Vinícius Carvalho, que "*altera o Marco Civil da Internet, Lei no 12.965, de 23 de abril de 2014, dispondo sobre a guarda dos registros de conexão à internet de sistema autônomo*", é mencionado nos seguintes trechos:

- Item 2.4.2 – "*Guarda dos registros de conexão por todos os provedores de internet e migração para o IPv6 ou tecnologia similar*" da sub-relatoria de Segurança Cibernética no Brasil, do deputado Rodrigo Martins. (pág 137);
- Item b) na seção "3 – Proposições Legislativas em Tramitação na Câmara cuja discussão se mostra importante";
- Item nº 13 das Conclusões do Relator, deputado Espiridião Amin (pág 163).
- Sub-item ii) do item nº 22 das Conclusões do Relator, deputado Espiridião Amin (pág. 168).
- Item b) da seção "*5 – Recomendações e Encaminhamentos da Comissão*"

Sugerimos remover, da lista de projetos de lei cujo debate têm reconhecida importância, a menção ao PL nº 3237/15, cuja finalidade é *aumentar* o alcance da retenção de dados. A proposta desse projeto de lei viola direitos fundamentais como a privacidade e a liberdade de expressão, conforme diversas pessoas da academia e da sociedade civil que se manifestaram presencialmente nesta CPI, além da Corte Interamericana de Direitos Humanos, da Corte de Justiça Europeia e de Relatores Especiais das Nações Unidas. Não há estatísticas ou estudos que justifiquem andar nesta direção, tendo havido apenas indicações anedóticas na fala de delegados e outros representantes de setores policiais ou investigativos.

Registre-se que não foi o Marco Civil da Internet o documento responsável por definir o conceito de "*Administrador de Sistema Autônomo*" (AS). A definição mencionada no art. 5º, IV, da Lei nº 12.965/2014 incorpora a classificação já existente e reconhecida internacionalmente por meio dos *Request for Comments* (ou "pedido de comentários"), documentos técnicos desenvolvidos pela *Internet Engineering Task Force*, instituição que especifica os padrões técnicos a serem implementados e utilizados em toda a internet. O Marco Civil apenas incluiu

no ordenamento jurídico brasileiro um conceito técnico já concebido e aplicado na prática, espelhando a maneira como a internet se estrutura e organiza sua dinâmica.

Assim, propor a alteração desse conceito para incluir qualquer provedor de conexão à Internet, desde que preste serviço ao público em geral, constitui uma imprecisão sem paralelo nos padrões técnicos aplicados à rede.

Além disso, o problema do referido projeto de lei não é só técnico, mas substantivo.

Primeiro, obrigar todo provedor de conexão a guardar todos os registros de conexão durante um ano implica grande custo de armazenamento seguro desses dados. Centros comunitários de acesso e outras iniciativas semelhantes, muito relevantes para a concretização dos princípios previstos no Marco Civil, seriam prejudicadas e até descontinuadas.

Em segundo lugar, a retenção de dados não é bema ceita no âmbito internacional. Conforme uma tabela de comparação feita pela empresa australiana PureVPN, referente a outubro de 2015, apenas 17 países, entre União Europeia e EUA, têm alguma lei que obrigue a guarda de registros de conexão, e 8 deles estão sob questionamento por recurso, revisão ou ação judicial. Alguns países europeus ainda estão tendo que retirar as previsões de seus ordenamentos jurídicos, desde que a retenção de dados foi julgada inconstitucional pela Corte de Justiça Europeia em 2014, por violação do direito fundamental à privacidade.

Na América Latina, a retenção de dados também é polêmica. Em todos os países onde foi proposta ou adotada, a medida encontrou forte repúdio da sociedade civil e de internautas: no Paraguai, houve a campanha contra a #Pyrawebs <https://www.apc.org/es/node/20630/>; no Peru, a #LeyStalker <https://antivigilancia.org/pt/2015/11/lei-stalker-no-peru/>. Aqui no Brasil a obrigação da guarda de registros do Marco Civil da Internet também foi criticada, sendo "um dos pontos mais polêmicos desta discussão", como documentado no site da primeira consulta pública do MCI <http://culturadigital.br/marcocivil/category/consulta/1-direitos-individuais-e-coletivos-eixo-1/1-1-privacidade/1-1-3-guarda-de-logs/>.

O Conselho de Direitos Humanos das Nações Unidas publicou o relatório "The Right to Privacy in the Digital Age" ("privacidade na era digital") <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf>, no qual afirma que a retenção de dados interfere na privacidade até mesmo quando os dados nunca são usados – no caso, referindo-se aos programas de vigilância em massa da agência de segurança nacional dos EUA, a NSA (tradução e grifo nosso):

Segue disso que qualquer captura de dados de comunicação é potencialmente uma interferência na privacidade e, além disso, que a coleta e retenção de dados de comunicações significa uma interferência com a privacidade quer ou não estes dados sejam posteriormente consultados ou usados. Mesmo a mera possibilidade das informações de comunicação serem capturadas cria uma interferência com a privacidade, com um efeito desencorajador (chilling effect) em direitos, incluindo aqueles à liberdade de expressão e associação. A própria existência de um programa de vigilância em massa então cria uma interferência com a privacidade.

Por fim, vale explicitar que todo endereço IP está ligado a um administrador de sistema autônomo, mesmo que não haja uma relação prestador-cliente entre o AS e o usuário final. Diante de um pedido ao AS, com a devida ordem judicial, será possível identificar a rede ou mesmo a máquina/dispositivo em que o IP suspeito foi utilizado, dando elementos importantes para a continuidade das investigações (na grande maioria dos casos será possível, por exemplo, saber quando e em que local o IP foi utilizado). É assim que "crimes offline" são normalmente investigados. Não é porque a Internet tecnicamente nos permite controlar de perto a vida e as condutas de cada um, o que poderíamos fazer também no mundo offline se implantássemos chips em todos os cidadãos, que lançaremos mão de medidas que afrontam diretamente o direito à privacidade e à liberdade de expressão.

Considerações finais

Seguimos à disposição para quaisquer futuras eventualidades no encerramento dos trabalhos desta Comissão, bem no debate de propostas normativas relacionadas.

Brasília, 22 de abril de 2016.

Lucas Teixeira, Diretor Técnico e
Joana Varon, Diretora Geral
Coding Rights
joana@codingrights.org (21) 98689-1313
lucas@codingrights.org (21) 99968-5003

Paulo Rená, chefe executivo de pesquisa
Instituto Beta: Internet e Democracia - IBIDEM
paulo@ibidem.org.br (61) 8334-3055

Veridiana Alimonti, Jonas Valente e Bia Barbosa
Intervozes - Coletivo Brasil de Comunicação Social
bia@intervozes.org.br (61) 9951-4846