RIO DE JANEIRO, 03 MAIO DE 2016

*Versão revisada e atualizada*

## Contribuição Técnica

# CPI de Crimes Cibernéticos

*Contribuição do ITS Rio ao relatório da CPI-CIBER*

Análise revisada e atualizada do ITS sobre a terceira versão do relatório da CPI dos cibercrimes, divulgado 26 de abril e a "nota de esclarecimento".

ITS
Instituto
de Tecnologia
& Sociedade
do Rio

## Introdução

Diante da publicação da terceira versão do relatório da CPI dos Cibercrimes e da "nota de esclarecimento" com proposta de novo projeto de lei para tratar do bloqueio de aplicações e conteúdos na internet, o Instituto de Tecnologia e Sociedade do Rio vem apresentar versão revisada e atualizada de sua análise sobre os temas propostos pela CPI que afetam diretamente os pilares do Marco Civil da Internet e o funcionamento da Internet no Brasil.

## Sobre

O Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio) é uma instituição de pesquisa dedicada ao desenvolvimento de projetos sobre o impacto social, jurídico, cultural e político das tecnologias de informação e comunicação. Com ampla atuação internacional, derivada da experiência e trabalho acumulado por mais de 15 anos por parte dos seus fundadores, o ITS realiza pesquisas orientadas ao atendimento do interesse público e que gerem reflexões e propostas para avançar o diálogo democrático, a proteção dos direitos humanos e a produção de impactos relevantes na formação e execução de políticas públicas e práticas privadas. Formado por professores e pesquisadores de diversas instituições de ensino e pesquisa como a UERJ, PUC-Rio, FGV, IBMEC, ESPM, MIT Media Lab, dentre outras, o ITS conta com uma rede de parceiros nacionais e internacionais e tem, dentre os seus focos de atividade, os debates sobre privacidade e dados pessoais, direitos humanos, governança da internet, novas mídias, comércio eletrônico, inclusão social, educação digital, cultura e tecnologia, propriedade intelectual, tecnologia e democracia, dentre outros temas.

# Sumário

## O Combate ao Cibercrime no Brasil:
## A Lei Brasileira Já Foi Modificada para Cobrir a Questão

A busca pelo combate aos atos criminosos praticados por meio da internet é objetivo legítimo e de grande importância. No entanto, nos últimos anos, com o advento da internet e da tecnologia digital, **a legislação brasileira já passou por uma intensa reforma voltada especificamente ao combate aos cibercrimes.** Nesse sentido, foi aprovada a Lei 10.695 de 2003, resultado de intensos trabalhos realizados pela **CPI da Pirataria.** Essa lei alterou dispositivos essenciais do Código Penal brasileiro com relação à punição de crimes relativos à propriedade intelectual e, notadamente, os direitos autorais. Com isso, o Código Penal foi atualizado para lidar com novos delitos contra os direitos autorais no ambiente digital, tendo havido ainda o aumento de penas e a criação de situações agravantes, relacionadas às novas tecnologias.

Já em 2008, houve a aprovação da Lei 11.829 de 2008, que foi resultado por sua vez dos intensos trabalhos promovidos pela **CPI da Pedofilia** e alterou o Estatuto da Criança e Adolescente, criando especificamente todo um aparato jurídico para o combate a essa nefasta prática, que contou, dentre outras medidas, com a criminalização da aquisição e posse de material de pornografia infantil e outras condutas relacionadas à pedofilia na internet.[1] A esse respeito, o presidente da Safernet (entidade que mais tem lutado pelo combate à pedofilia no Brasil), o advogado Thiago Tavares, declarou ao jornal Folha de São Paulo em 2 de abril de 2016, ao ser perguntado a respeito do relatório da presente CPI dos Cibercrimes, entender não ser mais necessária qualquer modificação legislativa no Brasil para o combate da pedofilia na internet, afirmando ser "contra o resultado apresentado pelos deputados". Em suas palavras, publicadas pelo jornal: "a lei 11.829, resultante da CPI da Pedofilia, de 2008, já tipificou como crime qualquer publicação de conteúdos pornográficos impróprios contra crianças".[2]

---

*1 Em relação à pornografia infantil, o relator especial da ONU para liberdade de expressão, Frank La Rue, reconhece a gravidade do tema, mas alerta que os estados devem focar seus esforços em identificar os responsáveis pela produção e disseminação do conteúdo pedófilo ao invés de apenas se concentrar no bloqueio de conteúdo. Relatório do Relator Especial da ONU para Liberdade de Expressão, Frank La Rue, 16 de maio de 2011, par. 71: "Thus, by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realization of a range of other human rights."*
*Disponível em: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*

*2 www.folha.com.br/tec/2016/04/1756692-propostas-de-cpi-sobre-crimes-na-rede-sao-vistos-como-tentativa-de-censura.shtml*

Já em 2012, depois de um debate a respeito da chamada "Lei Azeredo" que durou mais de 5 (cinco) anos, foi proposta e aprovada a Lei 12.737 de 2012, popularmente conhecida como **Lei Carolina Dieckmann**. Essa lei dispôs sobre a tipificação criminal dos chamados "delitos informáticos", criando modalidades criminais próprias para os crimes na internet. Desde já adiantamos que, na visão do ITS, essa lei foi muito feliz em alcançar o devido equilíbrio entre o combate aos crimes digitais, ao mesmo tempo em que conseguiu reduzir eventuais efeitos colaterais relativos às condutas tipificadas, devendo ser preservada sua redação.

Por fim, esse amplo conjunto de modificações legislativas direcionadas ao combate dos cibercrimes foi ainda mais avançado em 2014, com a aprovação do **Marco Civil da Internet**. Como se sabe, trata-se de lei amplamente celebrada, tanto no Brasil quanto no plano internacional, por sua formulação precisa de direitos e deveres na internet, **prevendo, dentre várias questões, uma ferramenta poderosíssima para o combate dos delitos virtuais, qual seja: a obrigação da guarda de logs de conexão e logs de acesso de todos os usuários da internet brasileiros, pelo prazo de 1 (um) ano e 6 (seis) meses respectivamente.** Trata-se de medida que confere às autoridades de investigação civil e criminal um mecanismo sem precedentes no diz respeito à investigação e instrução processual penal. Por meio desses logs, é possível investigar crimes e delitos cometidos no passado, sendo possível analisar complexas relações entre usuários e redes criminosas. Esses "metadados", que o Marco Civil obriga a guardar, são inegavelmente a ferramenta de investigação mais forte (para não dizer invasiva) já criada no âmbito do direito brasileiro.

Não discutiremos neste relatório todas as implicações jurídicas da adoção desse modelo pelo Brasil, mas vale dizer que na Europa, esse modelo de guarda e retenção de dados dos usuários foi julgado como inconstitucional pela Corte de Justiça Europeia e por vários países da União Europeia, por sua invasividade e ameaça à privacidade e outros direitos fundamentais. No momento ainda diversos países da União Europeia estão revisando as suas legislações nacionais sobre guarda de dados de forma a aperfeiçoar o combate à ilícitos e ao mesmo tempo respeitar a privacidade e a proteção de dados pessoais . Justamente por isso não parece adequado que se alterem as regras já estabelecidas no Brasil sobre esse tópico através de projetos de lei de vertente criminal. Tudo isso, apesar daquele continente enfrentar a grave e abominável ameaça do terrorismo.

Em todo caso, ressalta-se uma vez mais que esse modelo invasivo, e amplamente poderoso, encontra-se em vigor hoje no Brasil e à disposição das autoridades de investigação e de instrução processual penal ou mesmo civil. Além dessas poderosas ferramentas, o Marco Civil criou também várias outras medidas para o combate aos delitos virtuais, dentre elas a responsabilização subsidiária de provedores de aplicação de internet, obrigando-os a retirar materiais contendo cenas de nudez ou atos sexuais indevidos ("pornografia de vingança") após recebimento de notificação da vítima.

Com isso, gostaríamos de salientar uma vez mais que a lei brasileira já passou por intensa reforma nos últimos anos no intuito de se combater os cibercrimes. Juntamos a essa observação o fato de que o combate aos delitos, cometidos tanto na internet como fora dela, deve sempre observar as garantias constitucionais e os direitos fundamentais, tais como a presunção de inocência, o devido processo legal, o princípio do juiz natural, o direito à privacidade e ao sigilo das comunicações, a liberdade de expressão, dentre vários outros,

Entendemos desde já que muitas propostas formuladas pela CPI dos Crimes Digitais não apenas são desnecessárias, haja vista a ampla modificação da legislação brasileira dos últimos anos, como são desproporcionais. Além disso, entendemos que as propostas ferem as garantias constitucionais listadas no parágrafo anterior. Seu efeito prático, em nossa análise, equivale à propositura de um sistema de controle e censura da internet, que pouco guarda conexão ao combate aos cibercrimes, já amplamente cobertos pela legislação brasileira.

Abaixo desenvolvemos em maiores detalhes essas considerações.

## 1. O acesso livre à internet é essencial para o exercício da cidadania

O acesso à internet, por conta da sua importância para a vida contemporânea, foi apontado como um direito fundamental pela Organização das Nações Unidas (ONU), na medida em que se torna requisito para a realização de outros direitos essenciais (dentre eles, a liberdade de expressão). [3] Nas palavras do Relatório Especial da ONU sobre a Liberdade de Expressão, publicado em 2011: "Ao contrário de qualquer outro meio, a Internet permite que os indivíduos busquem, recebam e difundam informações e ideias de todos os tipos de forma instantânea e barata para além das fronteiras nacionais". [4]

A internet é hoje o meio privilegiado para o exercício de outros direitos humanos e da cidadania, além de estimular o desenvolvimento econômico, social e político, e contribui para o progresso humano. Além disso, a internet livre conecta-se diretamente com a democracia e com o Estado Democrático de Direito. O respeito a uma rede livre de influência e interferências externas passou a se configurar como um importante indicador para se avaliar o grau de respeito à democracia e ao império da lei em diversos países. Esse entendimento foi incorporado ao ordenamento jurídico brasileiro por força do Artigo 7º do Marco Civil da Internet, que determina que "o acesso à internet é essencial ao exercício da cidadania".

Assim, qualquer mudança legislativa que impacte a internet – infraestrutura essencial para todos os países contemporâneos - deve ser amplamente debatida com a sociedade. Qualquer interferência na rede deve demonstrar que os benefícios desta são maiores que seus efeitos colaterais. Essas interferências devem ser feitas baseadas em dados empíricos e sempre se ouvindo os vários setores da sociedade: setor público, setor privado, comunidade técnica e acadêmica, terceiro setor e assim por diante.

Além disso, o caráter essencial da internet deve afastar de pronto qualquer possibilidade de intervenção ou bloqueio em sua infraestrutura técnica. Não se admite bloquear diretamente na

*3 Relatório do Relator Especial da ONU para Liberdade de Expressão, Frank La Rue, 16 de maio de 2011, par. 22: "Thus, by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realization of a range of other human rights."Disponível em: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*

*4 Relatório do Relator Especial da ONU para Liberdade de Expressão, Frank La Rue, 16 de maio de 2011, par. 22: "Thus, by acting as a catalyst for individuals to exercise their right to freedom of opinion and expression, the Internet also facilitates the realization of a range of other human rights."Disponível em: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*

camada da infraestrutura da rede qualquer tipo de conteúdo. Nesse sentido, a título ilustrativo, considerando-se que a internet é serviço tão essencial quanto eletricidade, fornecimento de água ou os correios, não se admite qualquer interferência no funcionamento desses serviços. Da mesma forma como não se "desliga a eletricidade" de uma determinada casa porque ali habita um criminoso, ou se suspende o fornecimento daquele domicílio, ou ainda, a entrega de cartas (fazer isto atentaria contra o princípio da dignidade da pessoa humana), não se "desliga" partes da internet. Tal desligamento seria, igualmente, atentar contra a essencialidade da rede para a vida humana contemporânea.

## 2. A Internet deve ser vista como fator para o desenvolvimento econômico, a geração de empregos e a inovação, e não apenas como um "covil de criminosos"

A internet, além de ser considerada essencial ao exercício da cidadania, passou a ser também de suma importância para o desenvolvimento econômico dos países. A esse respeito, há um dado positivo com relação ao Brasil que deve ser considerado. Nosso país é apontado como um dos países mais empreendedores do mundo [5] e a internet desempenha um papel fundamental nisso. As "startups" (empresas de tecnologia que ambicionam crescer vigorosamente) brasileiras estão gerando empregos e inovação, com dados amplamente positivos, colhidos pela Associação Brasileira de Startups. A esse respeito, o setor já movimenta hoje alguns bilhões de reais, e vem se expandindo ao longo dos últimos dois anos, apesar da crise. [6]

As startups atuam cada vez em segmentos como mídias sociais, e-commerce, pagamentos eletrônicos, mídia, conteúdo, de games, software e hardware, mensagens eletrônicas, fintech (finanças) entre vários outros. A internet é, portanto, um elemento central para o desenvolvimento futuro do país.

A partir daí, ressaltamos que **não se regula a internet "em tiras".** Uma regulamentação sobre a rede, como essa que propõe a CPI dos Crimes Cibernéticos, **tem impacto sobre todo o ecossistema da internet.** Em outras palavras, ao propor um conjunto de medidas que responsabilizam provedores,

5 *De acordo com pesquisa divulgada pelo Sebrae com o resultado da pesquisa mundial do GEM (Global Entreperneurship Monitor) de 2014.*

6 *http://www.abstartups.com.br/*

intermediários, que interfere no funcionamento da infraestrutura da rede, que aumenta os custos de compliance das empresas de internet, as propostas da CPI implicarão em um significativo aumento do chamado **Custo Brasil** com relação às empresas de tecnologia do país. Nossa preocupação é especialmente direcionada às empresas brasileiras, principalmente aquelas de pequeno e médio porte. Bem ou mal, as grandes empresas estrangeiras de tecnologia que atuam no país podem absorver o impacto do aumento do Custo Brasil derivado das mudanças regulatórias propostas pela CPI.

Já o empresário brasileiro de pequeno e médio porte, que não possui recursos para investir em advogados, em funcionários para "patrulhar" a rede, em um departamento de compliance para verificar e fornecer dados requisitados pelas autoridades de investigação, esse irá ser impactado fortemente. Em outras palavras, além da dimensão de direitos que serão afetados pelas propostas da CPI dos Crimes Cibernéticos, haverá também um enorme aumento de custos com advogados, funcionários, monitoramento, organização, busca e fornecimento de informações para autoridades. Esse impacto deixará as empresas brasileiras em posição de desvantagem com relação àquelas que atuam globalmente e possuem estrutura de capital suficiente para suportar esses custos. Em outras palavras, as propostas formuladas pela CPI impactam negativamente, para além de todas as questões de direitos fundamentais aqui apontadas, a competitividade do empresário brasileiro na rede.

Sendo assim, o Congresso brasileiro não pode apenas olhar para a internet como um espaço para a prática de atos criminosos, como fez o relatório da CPI dos Crimes Cibernéticos. Ao contrário, a rede deve ser reconhecida por sua promoção ao empreendedorismo inovador, fundamental para que o país construa novos modelos de desenvolvimento. Não se pode ignorar os impactos negativos para o desenvolvimento da internet, do país e da sociedade brasileira se esses projetos de lei forem aprovados. Essas mudanças aumentariam o Custo Brasil e, em última análise, contribuiriam para isolar o país do mercado global, na medida em que desestimularia empresas globais de tecnologia a abrirem escritórios em nosso país, caso leis exorbitantes como as propostas por esta CPI venham a ser aprovadas. Esse é o pior dos mundos, inclusive do ponto de vista das perdas tributárias ocasionadas.

## 3. A Necessidade de se manter a legislação do país equilibrada em consideração aos objetivos legítimos de proteção aos direitos fundamentais e a instrução processual penal

Vale lembrar que o Marco Civil da Internet, justamente pelo ensejo de se alcançar o equilíbrio e proporcionalidade entre direitos e deveres, tornou-se um modelo celebrado internacionalmente. O Marco Civil serviu e serve de inspiração para outros países na adoção de instrumentos jurídicos semelhantes dedicados à matéria, como foi o caso recente da Itália. [7] No plano internacional, o Marco Civil representa um dos poucos campos em que o país é ainda reconhecido positivamente nesses tempos conturbados. Abdicar dessa posição de liderança global no campo da regulação da internet afeta negativamente a inserção do país no âmbito da política externa.

De modo geral, as propostas legislativas da CPI dos Cibercrimes (analisadas abaixo), se aprovadas, introduzirão em nosso país práticas típicas de países autoritários, que censuram e controlam a internet. Essas propostas levarão à possibilidade de criminalização de atos triviais, praticados por milhões de usuários da rede. Vale ainda notar que a tendência mais moderna do Direito Penal Brasileiro vem buscando a implementação de novos mecanismos de política criminal, que possam ir além da criminalização e do aumento de penas.

Nesse sentido, nosso entendimento é que o combate aos cibercrimes, para ser efetivo, precisa ser multissetorial. Isto é, precisa contar com o envolvimento do setor público, do setor privado, da comunidade técnica e acadêmica, do terceiro setor e assim por diante. O direito penal não é o instrumento adequado para a promoção a cooperação entre esses diversos setores. Ao contrário, a mera e simples criminalização pode gerar antagonismos entre esses setores e desincentivos para que haja uma cooperação efetiva.

Se forem aprovados os projetos de lei propostos pelo relatório - bem como aqueles outros já em tramitação e por ele apoiados - haverá um desequilíbrio no ordenamento jurídico brasileiro, configurado pela **sobrerregulação** da internet. Essa sobrerregulação, além de todo o impacto negativo para o campo dos direitos mencionados acima, desestimula a inovação e o empreendedorismo brasileiro.

---

*7 Sobre o tema ver http://www.lindro.it/la-carta-dei-diritti-internet-le-leggi-della-rete/. Acesso em 06.04.2016*

A seguir apresentamos nossos comentários a respeito de propostas específicas de mudança legislativa formuladas pela CPI dos Crimes Cibernéticos. Rogamos respeitosamente que os elementos apresentados aqui sejam levados em consideração pelos membros da CPI.

Nossa sugestão é de que a CPI recomende ao portal E-Democracia da Câmara dos Deputados que submeta os textos legais que estão sendo propostos a uma consulta pública aberta na internet, tal como esse mesmo portal fez com o Marco Civil da Internet. Acreditamos que a ampliação do debate para o maior número de setores da sociedade, incluindo-se usuários, empresas de tecnologias brasileiras, startups do país, investidores, órgãos de defesa do consumidor, setor acadêmico, comunidade técnica e científica, setor privado e assim por diante, traria importantes insumos para a formulação de uma proposta construtiva para o momento atual do ordenamento jurídico do país.

Passamos assim à análise das proposições legais formuladas pela CPI dos Cibercrimes.

## Análise do ponto 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

A modificação proposta, para alterar o art. 154-A, mudando "invadir", que quer dizer "assenhorar-se", "apropriar-se" de algo de terceiro como se seu fosse, por "acessar" que significa "ter acesso a algo", mostra claramente a amplitude do tipo penal que se está propondo. O "acesso" é a ação fundamental da internet. Todo e qualquer usuário "acessa" a rede, um site, um aplicativo. **Entendemos que definir um tipo penal cujo elemento central é a ação de "acessar" é algo perigoso e que atenta à boa técnica legislativa.** Isso se dá mesmo que o tipo "acessar" a ser criminalizado esteja qualificado logo a seguir. O fato é que todo e qualquer usuário brasileiro acessa a internet. Por essa razão, o vocábulo "invadir", como se encontra hoje no tipo penal atual definido pela "Lei Carolina Dieckmann", é muito mais adequado e prudente do que o tipo "acessar", excessivamente vago e abrangente.

Ademais, a redação atual do artigo 154-A é muito superior à redação proposta pela CPI dos Crimes Cibernéticos. O artigo atual prevê que a invasão somente terá consequências se o seu fim for *obter, adulterar ou destruir dados ou informações ou instalar vulnerabilidades para obter vantagem ilícita.*

Já a nova redação não exige qualquer tipo de prejuízo ou fim ilícito, o que possibilitaria a interpretação de que alguma utilização de sistema informatizado - culposo, ou seja, sem a intenção de fazê-lo - de forma que contrariasse, por exemplo, seus *"termos de uso"*, poderia ensejar a prática de um delito com pena de detenção de até 01 ano e multa. O requisito de causar prejuízo (que na forma proposta passaria para o § 2º do art. 154-A) seria apenas causa agravante de pena e não mais requisito para o tipo penal e o requisito de obtenção de fim ilícito sequer existiria na nova redação proposta.

Vê-se, assim, que o novo tipo penal que se propõe é tão amplo que poderá abarcar situações que não deveriam ser definidas como crime ou que até mesmo não tragam qualquer prejuízo para a "vítima" do acesso ou vantagem para aquele que cometer esse "delito", o que demonstra uma criminalização exagerada de uma conduta que não deveria ser enquadrada sequer como um ilícito civil, quanto mais penal.

**<adicionado com base na 3a versão do relatório CPI Ciber>**

Destaque-se que na terceira versão do relatório da CPI incluiu na justificativa da proposta de PL que "A proposta exige para a configuração do delito, porém, que os dados informatizados sejam expostos a risco de divulgação ou de utilização indevidas, o que afasta a tipicidade de condutas que não possuem qualquer ofensividade, como a simples violação de "termos de uso", por exemplo." Esse argumento, com a devida venia, nao reflete a realidade, já que o tipo penal apenas exige o acesso indevido e por qualquer meio, o que ja transforma a conduta em delito, nao havendo necessidade de que haja outro dispositivo legal a enquadra-la como delituosa. Assim, insistimos que o texto proposto apresenta uma criminalização exagerada e pode sim enquadrar como delitos situacoes que sequer deveriam ser tratadas como ilícito civil, ja que este exige a prova do dano.

Por fim, alertamos que vem circulando a afirmativa de que "a Lei Carolina Dieckmann não serviria para punir sequer o que ocorreu com a atriz Carolina Dieckmann". Essa afirmação é claramente falsa e recomendamos que tal afirmação seja suprimida do relatório final da CPI dos Cibercrimes para que esse documento não incorra em descrédito. A ação que foi aplicada à atriz Carolina Dieckmann é completamente passível de punição pelo tipo penal em comento, na medida em que os perpetradores da ação contra a atriz incorreram em **"invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, com o fim de obter dados ou informações sem autorização expressa ou tácita do titular".** Essa conduta está precisamente tipificada na Lei Carolina Dieckmann, da seguinte forma:

*Art. 154-A. Invadir 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 instalar vulnerabilidades para obter vantagem ilícita:*

Logo, nosso entendimento é que o tipo penal atualmente em vigor no ordenamento jurídico brasileiro é não só suficiente para coibição do cibercrime em comento, como também adequado do ponto de vista de sua formulação legal, preocupando-se com o necessário equilíbrio entre abrangência e

especificidade do tipo.

**RECOMENDAÇÃO À CPI DOS CIBERCRIMES:**

Supressão integral da proposta formulada e manutenção de legislação atual em vigor, que é perfeitamente adequada à sua finalidade.

## Análise do ponto 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.

Uma das principais garantias do Marco Civil da Internet é o **respeito ao devido processo legal e ao princípio do juiz natural.** Essas salvaguardas são essenciais, dentre outras coisas, para assegurar a liberdade de expressão na internet. Em atenção a esses três princípios, o provedor de aplicações de internet somente será responsabilizado por conteúdo gerado por terceiro após ser-lhe determinado por **decisão judicial** a retirada do conteúdo. Afastar o controle judicial para retirar conteúdo que atente contra a honra de maneira acintosa é violar o princípio do devido processo legal, do juiz natural (isso transformaria os próprios provedores em juízes capazes de decidir quais conteúdos são ilícitos ou não) e a liberdade de expressão.

Entendemos que o mesmo problema apontado acima persiste com relação à exigência de que haja a remoção automática de conteúdos que já tenham sido objeto de ordem judicial. Como ensina a Teoria Geral do Processo, a decisão judicial possui efeitos específicos, delimitados especificamente entre as partes do processo. Pretender estender o efeito de uma ordem judicial específica para além desses limites configura-se como um desvirtuamento do processo civil e criminal brasileiro.

### <adicionado com base na 3a versão do relatório CPI Ciber>

A nova redação proposta na terceira versão do relatório da CPI de Cibercrimes para o novo art. 21-A e do §1º faz com que os provedores tenham que atender a notificações privadas para remover conteúdo idêntico, objeto de uma ordem judicial de retirada de conteúdo, cabendo aos mesmos conferir a "validade da ordem judicial em questão e a verificação da legitimidade para apresentação do pedido." Uma vez mais, isso transforma os provedores de internet em juízes, com a atribuição de decidir no caso concreto quais conteúdos seriam identicos, se a ordem judicial prévia se aplicaria a eles, e mais, se o requerente da retirada do conteudo teria legitimidade para tanto.

Isso viola, uma vez mais, o devido processo legal e o princípio do juiz natural. Apenas um juiz poderia decidir os contornos de tal situação no caso concreto. Delegar essa atribuição aos provedores de internet, é temerário e afronta tais princípios constitucionais.

**<adicionado com base na 3a versão do relatório CPI Ciber>**

Destaque-se que a parte final do novo art. 21-A preve que se o provedor atender a solicitaçao de retirada de conteudo alegadamente idêntico a conteúdo objeto de decisão judicial anterior no prazo previsto neste dispositivo "não poderá ser responsabilizado pelas consequências da eventual falta de correspondência entre os conteúdos", o que estimularia, evidentemente, que os provedores retirem todo o conteúdo alegadamente idêntico para afastar qualquer risco de responsabilização, já que nesta hipótese aplicar-se-lhes-á a salvaguarda prevista na parte final do dispositivo em questão.

O artigo 19 do Marco Civil da Internet já criou um sistema de remoção de conteúdo na rede que prestigia o Poder Judiciário como instância legítima para decidir sobre a licitude ou a ilicitude de um determinado conteúdo. Ao abrir a possibilidade de que particulares passem a notificar extra-judicialmente os provedores para remover conteúdos que possam ser idênticos, o PL proposto cria uma zona de incertezas que não apenas fragiliza os direitos das vítimas, que passarão a contar com um mecanismos cheio de subjetividades e pouco eficiente (no qual se questiona se o conteúdo é mesmo idêntico), como ainda fragiliza também a posição do provedor, que pode optar por simplesmente remover tudo o que for objeto de notificação ou contestar a pretensa identidade de conteúdos, ficando assim sujeito a futuros questionamentos judiciais.

Não nos parece devido nesse momento modificar o sistema de responsabilização e remoção de conteúdo já previsto no artigo 19 do Marco Civil.

Especialmente porque essa medida vai em sentido totalmente oposto à jurisprudência consolidada do Superior Tribunal de Justiça, que, com relação aos motores de busca, firmou entendimento no sentido de que "não se pode, sob o pretexto de dificultar a propagação de conteúdo ilícito ou ofensivo na web, reprimir o direito da coletividade à informação. Sopesados os direitos envolvidos e o risco potencial de violação de cada um deles, o fiel da balança deve pender para a garantia da liberdade de informação assegurada pelo art. 220, § 1º, da CF/88, sobretudo considerando que a Internet representa, hoje, importante veículo de comunicação social de massa." [8] Nesse sentido, vale citar decisão recente do

8 *Resp 1.316.921—RJ. Relatora Ministra Nancy Andrighi. 3a Turma, Julgado em 26 de junho de 2012.*

STJ, em abril de 2016, na qual ficou assentado que "a jurisprudência do STJ, em harmonia com o art. 19, § 1º, da Lei nº 12.965/2014 (Marco Civil da Internet), entende necessária a notificação judicial ao provedor de conteúdo ou de hospedagem para retirada de material apontado como infringente, com a indicação clara e específica da URL - Universal Resource Locator". [9] Segundo o relator: "não se pode impor ao provedor de internet que monitore o conteúdo produzido pelos usuários da rede, "de modo a impedir, ou censurar previamente, a divulgação de futuras manifestações ofensivas contra determinado indivíduo". [10]

**A impossibilidade de censura prévia na internet também pode ser identificada no posicionamento do Supremo Tribunal Federal,** em especial na ADPF 130, na qual o Tribunal entendeu que *"silenciando a Constituição quanto ao regime da internet (rede mundial de computadores), não há como se lhe recusar a qualificação de território virtual livremente veiculador de ideias e opiniões, debates, notícias e tudo o mais que signifique plenitude de comunicação".* [11] Parece-nos assim, que a proposta de PL apresentada, além dos problemas já apontados, padece de vício de constitucionalidade.

## RECOMENDAÇÃO À CPI DOS CIBERCRIMES:

Supressão integral da proposta legislativa. Alternativamente, supressão integral do trecho do artigo contendo a expressão: *"que contenha parte majoritária do conteúdo original e que continue a configurar a característica considerada como infringente".*

---

*9 Terceira Turma revê punição a provedor de internet por material ofensivo, 12.04.2016, Disponível em: http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/Not%C3%ADcias/Not%C3%ADcias/Terceira-Turma-rev%C3%AA-puni%C3%A7%C3%A3o-a-provedor-de-internet-por-material-ofensivo*

*10 Terceira Turma revê punição a provedor de internet por material ofensivo, 12.04.2016, Disponível em: http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/Not%C3%ADcias/Not%C3%ADcias/Terceira-Turma-rev%C3%AA-puni%C3%A7%C3%A3o-a-provedor-de-internet-por-material-ofensivo*

*11 ADPF 130, rel. min. Ayres Britto, julgamento em 30–4–2009, Plenário, DJE de 6–11–2009.*

## Análise do ponto 1.6:

### PROJETO DE LEI QUE POSSIBILITA O BLOQUEIO DE APLICAÇÕES DE INTERNET POR ORDEM JUDICIAL, NOS CASOS EM QUE ESPECIFICA

**<adicionado com base na 3a versão do relatório CPI Ciber>**

A Câmara dos Deputados publicou no dia 28/04/2016 uma "nota de esclarecimento" alterando a redação de uma das propostas mais polêmicas da CPI: **a de mudar o Marco Civil para permitir o bloqueio completo de sites, na camada de infraestrutura, sem direito ao contraditório, e mais, antes mesmo de ser proferida sentença no processo no qual se determinaria o bloqueio.** Em outras palavras, censura pura e simples.

Em face às enormes críticas nacionais e internacionais que essa proposta recebeu, a nota divulgada na ultima sexta-feira pela Câmara altera a redação anterior fazendo algo simplesmente inacreditável. A nova redação equipara violação de direito de autor a atividades como "terrorismo", "exploração sexual de crianças", "crimes hediondos" e "tráfico internacional de armas". A proposta é de autoria dos deputados Rafael Motta (PSB-RN) e Sandro Alex (PSD-PR).

Ao colocar direitos autorais (e de propriedade industrial e intelectual) na mesma categoria do terrorismo, o que a CPI propõe é autorizar que qualquer juiz de primeira instância—sem as garantias do devido processo legal e da ampla defesa—possa simplesmente ordenar o bloqueio de sites, páginas na internet, redes sociais, ou aplicativos caso neles ocorra "violação de direito de autor". Em outras palavras, em havendo infração ao "copyright" em um site ou página na internet, a página poderá ser bloqueada diretamente na raiz da rede, afetando de uma só vez 200 milhões de brasileiros.

Como o direito autoral no mundo digital de hoje toca a vida de milhões de pessoas todos os dias, um político, se valendo da vaga e atécnica expressao "precipuamente dedicados", poderá facilmente utilizar a desculpa da "violação de seus direitos autorais" ou mesmo de seus "direitos de imagem" para solicitar o bloqueio a sites que falem mal deles na internet.

Em outras palavras, sites onde ocorre a utilização de vídeos, fotos e até trechos de discursos de

políticos para criticá-los, poderão ser bloqueados quando forem "precipuamente dedicados" à prática de violações de direito de autor e "não tiverem representação no Brasil".

**<adicionado com base na 3a versão do relatório CPI Ciber>**

Ora, não há que se falar em aplicação de internet dedicada precipuamente à prática de crimes, já que as aplicações são criadas e comercializadas para fins legítimos e o uso que alguns usuários fazem dessa aplicação é que podem ensejar alguma ilicitude, mas nunca a aplicação em si. Admitir isso seria o mesmo que admitir que se pudesse bloquear o uso do telefone no país ou mesmo fechar as rodovias, ja que diversas comunicações relativas à pratica de crimes se dão através de telefone e várias cargas ilicitas são transportadas pelas rodovias do país todos os dias, e ninguém em sua sã consciência cogitaria bloquear os telefones ou mesmo fechar as rodovias, até porque isso não impediria que o delitos continuassem a ser cometidos, apenas faria com que os criminosos se valessem de outros meios.

**<adicionado com base na 3a versão do relatório CPI Ciber>**

A proposta formulada pela CPI dos Cibercrimes de bloqueio de sites e aplicações diretamente na camada da infraestrutura da rede só encontra respaldo tipicamente, de fato, em países autoritários como Coreia do Norte, China, Arábia Saudita e outros países autoritários e tem um único objetivo: criar um verdadeiro muro na internet—um cordão sanitário—que isola a rede do país com relação a vários serviços e sites considerados "impróprios" para aquela população.

Entidades globais como a Electronic Frontier Foundation (EFF) já escreveram longamente sobre o uso dos direitos autorais como ferramenta de censura estatal. No artigo Copyright Law as a Tool for State Censorship of the Internet, a pesquisadora Maira Sulton diz claramente: *"Quando políticos e agentes estatais buscam censurar a internet, eles farão isso usando o método mais rápido e fácil disponível. Por exemplo, usando notificações de direitos autorais."*

No mesmo artigo ela descreve vários casos de uso dos direitos autorais para a censura:
*"Na Arábia Saudita, um show satírico no Youtube chamado Fitnah foi censurado quando o canal de televisão estatal daquele país exigiu a retirada de vários vídeos da série. A seguir, o direito autoral foi usado no Líbano*

*para remover conteúdos similares. No Equador, o escritório de advocacia Ares Right tem enviado pedidos de remoção de conteúdos da internet criticando políticos do país com base em direitos autorais desde 2014. A prática continua até os dias de hoje."*

Isso deixa claro o perigo da censura baseada nos direitos autorais. Se a CPI dos Cibercrimes for em frente com essa proposta, tal modelo levará à criação de um novo "Index" similar ao da Inquisição na Idade Média. A consequência é que haverá uma lista de sites, páginas e serviços que foram "bloqueados" da rede brasileira, impedindo que qualquer residente no país possa ter acesso a eles.

É claro que os direitos autorais são importantes. No entanto, o modelo proposto pela CPI, em vez de resolver as violações de direitos autorais em si mesmas, buscando os verdadeiros culpados, coloca a culpa na internet e pune os 200 milhões de brasileiros que serão impedidos de acessar determinados serviços na rede, abrindo espaço para abusos inaceitáveis.

Na internet brasileira (e de todos os países democráticos), vigora o princípio da chamada "inimputabilidade da rede", isto é, não se pode pôr a culpa na internet por crimes e violações que possam acontecer. Não se culpa a rede e ponto final! O princípio faz parte do Décalogo aprovado pelo Comitê Gestor da Internet para a governança da rede brasileira em 2009, que diz exatamente o seguinte:

*Inimputabilidade da rede*

*O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.*[12]

> Com isso, nossa recomendação para a CPI dos Cibercrimes é suprimir na íntegra toda e qualquer forma de bloqueio da rede, já que essa prática equivale à censura pura e simples e é típica de países autoritários.

12 *O Decalogo da Internet aprovado pelo Comite Gestor da Internet no Brasil esta disponivel em http://www.cgi.br/resolucoes/documento/2009/003 (Acesso em 01/05/2016).*

## <adicionado com base na 3a versão do relatório CPI Ciber>

A decisão tornada pública em 2 maio de 2016, na qual um juiz federal determina a suspensão do Whatsapp em todo o país por 72 (setenta e duas)[13] horas se tornará prática corriqueira se o PL proposto pela CPI dos Cibercrimes se tornar lei.

## <adicionado com base na 3a versão do relatório CPI Ciber>

Vale destacar que a nota de esclarecimento da CPI dos Cibercrimes volta a se valer do expediente de citar normas estrangeiras como exemplos de normas que autorizam o bloqueio de aplicaçoes da internet, quando na verdade tais normas não o autorizam da forma como propõe a CPI de Cibercrimes. A primeira norma citada é a Lei de Comunicaçoes de 2003 do Reino Unido (Communications Act of 2003), que na seção 132 citada na "nota de esclarecimento" prevê que somente poderá ser suspenso determinado serviço prestado em razão de uma ameaça à segurança pública ou à saúde pública ou por razões de segurança nacional, mas não nas hipóteses previstas no PL proposto na nota de esclarecimento, tanto que na mesma seção 132, em seu item 6, a referida lei prevê o pagamento de indenização ao provedor do respectivo serviço por danos a ele causados, o que deixa claro que o bloqueio, ou melhor, suspensão, nao se refere a qualquer prática do provedor do serviço, mas a ameaça à segurança pública ou à saúde pública ou à segurança nacional.[14]

---

*13 Folha de São Paulo. Justiça determina bloqueio do WhatsApp no Brasil por 72 horas. Disponível em http://www1.folha.uol.com.br/mercado/2016/05/1766869-justica-determina-bloqueio-do-whatsapp-em-todo-o-brasil-por-72-horas.shtml (Acesso em 02/05/2016).*

*14 132 Powers to require suspension or restriction of a provider's entitlement*
*(1)If the Secretary of State has reasonable grounds for believing that it is necessary to do so—*
*(a)to protect the public from any threat to public safety or public health, or*
*(b)in the interests of national security, (...)*
*(6)Those conditions may include a condition requiring the making of payments—*
*(a)by way of compensation for loss or damage suffered by the relevant provider's customers as a result of the direction; or*
*(b)in respect of annoyance, inconvenience or anxiety to which they have been put in consequence of the direction. A integra da Lei inglesa esta disponivel em http://www.legislation.gov.uk/ukpga/2003/21/section/132 (Acesso em 01/05/2016).*

**<adicionado com base na 3a versão do relatório CPI Ciber>**

O Código Penal Dinamarques, por sua vez, não traz qualquer autorização para o bloqueio de aplicações de internet, seja por disseminação de conteúdo relativo a pornografia infantil ou de qualquer outro conteúdo, ele apenas criminaliza tal prática, punindo os infratores com pena de no máximo 06 (seis anos).[15]

**<adicionado com base na 3a versão do relatório CPI Ciber>**

No que toca ao Código de Regulações Federais dos Estados Unidos (Code of Federal Regulations), no mesmo titulo 47, capítulo I, subcapítulo A, só que no item 8.5, veda-se o bloqueio de aplicações legais, [16] e não há que se dizer que uma aplicação de internet que venha a ser mal utilizada por alguns é uma aplicação ilegal. Muito pelo contrário, o que mostra é que essa norma igualmente não autoriza o bloqueio de aplicações simplesmente porque alguém as está utilizando para fins ilicitos. Autorizado estaria o bloqueio, por exemplo, de uma aplicação que treina alguém para cometer um crime, mas nunca de uma aplicação que tem por objetivo possibilitar a comunicação ou troca de mensagens e arquivos entre seus usuários. Esse mesmo raciocínio vale para a lei chilena também citada na "nota de esclarecimento" da CPI de Cibercrimes, que igualmente não autoriza o bloqueio de aplicações, muito ao contrário, ela veda de forma expressa qualquer tipo de bloqueio ou filtragem, conforme se infere da mera leitura da alínea 'a' de seu artigo 24-H.[17]

---

*15 §235 (1) Any person, who disseminates obscene photographs or films, other obscene visual reproductions or similar of persons under the age of 18, shall be liable to a fine or to imprisonment for any term not exceeding two years or in particularly aggravating circumstances to imprisonment for any term not exceeding six years. Considered as particularly aggravating circumstances are especially instances where the life of the child is endangered, where gross violence is used, where the child is caused serious harm, or instances of disseminations of a more systematic or organised nature. (2) Any person, who possesses or for a payment becomes acquainted with obscene photographs or films, other obscene visual reproductions or similar of persons under the age of 18, shall be liable to a fine or to imprisonment for any term not exceeding one year. (3) The provision in Subsection (2) does not include possession of obscene pictures of a person who has reached the age of 15, if the person has consented to the possession. O texto em ingles do Codigo Penal Dinamarques esta disponivel em http://www.unodc.org/tldb/pdf/Denmark_Criminal_Code_2005.pdf (Acesso em 01/05/2016).*

*16 §8.5 No blocking.*
*A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management. O texto do Codigo de Regulaçoes dos Estados Unidos esta disponivel em http://www.ecfr.gov/cgi-bin/text-idx?SID=c4ed955dbc10ac182c0b060efd6a0d76&mc=true&node=se47.1.8_15&rgn=div8 (Acesso em 01/05/2016).*

**<adicionado com base na 3a versão do relatório CPI Ciber>**

Voltamos a destacar, também, que o Regulamento 2015/2120 do Parlamento Europeu e do Conselho da União Europeia, novamente citado na "nota de esclarecimento" da CPI de Cibercrimes como exemplo de norma europeia que supostamente autorizaria o bloqueio de aplicações da internet, na verdade não traz qualquer previsao nesse sentido. Tal documento, que apenas reconhece a sujeição dos provedores de serviços a normas dos Estados-Membros que podem levar ao bloqueio de determinado conteúdo ou aplicação ilegal, estabelece, mesmo nessas hipóteses de conteúdo ou aplicação ilegal - o que, como destacado, não seria o caso de uma determinada aplicação que é mal utilizada para uma finalidade ilícita por alguns de seus usuários, já que a finalidade para a qual foi criada e comercializada é licita - um conjunto de salvaguardas obrigatórias aos estados-membros europeus, dentre elas os princípios da necessidade e da proporcionalidade e do devido processo legal, antes de efetuarem qualquer tipo de "bloqueio ou filtragem" em casos cuidadosamente especificados, requisitos estes que nao estao atendidos pela vaga e simploria redacao do §1° do novo art. 23-A proposta na "nota de esclarecimento" da CPI dos Cibercrimes. Não existe, assim, no ordenamento europeu, diferente do afirmado na "nota de esclarecimento" e na terceira versão do relatorio da CPI dos Cibercrimes, qualquer norma similar à que está sendo agora proposta pela CPI dos Cibercrimes que autoriza a qualquer juiz de primeira instância, "no curso do processo", bloquear diretamente na infraestrutura da rede qualquer site ou serviço de internet, afetando a vida de todos os brasileiros. Enquanto o documento Europeu estabelece uma série de salvaguardas e cautelas obrigatórias para os estados-membros, a proposta da CPI cria um "cheque em branco" para que a internet seja bloqueada no Brasil. [18]

---

*17 Ley 20.453/2010.*

*Art. 24-H*

*a) No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad al proveedor de acceso a Internet, según corresponda, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de éstos, habida cuenta de las distintas configuraciones de la conexión a Internet según el contrato vigente con los usuarios.*

*Disponivel em http://bcn.cl/1uzbi*

A proposta apresentada na "nota de esclarecimento" configura verdadeiro absurdo, vez que equipara a violação de direitos autorais a atos como "terrorismo", "pedofilia" e "crimes hediondos". Isso é, diga-se, um desrespeito às vítimas de crimes tão graves. Ao colocar o tema dos direitos autorais nessa mesma categoria, a CPI gera imensa perplexidade, pois parece estar mais preocupada em justificar a possibilidade de censura e controle da rede a qualquer custo do que efetivamente resolver a questão dos cibercrimes.

**RECOMENDAÇÃO À CPI DOS CIBERCRIMES:**

Supressão integral da proposta em comento.

1 *(13) Por um lado, em certas situações, os prestadores de serviços de acesso à Internet podem estar sujeitos a atos legislativos da União ou a legislação nacional conforme com o direito da União (referentes, por exemplo, à legalidade dos conteúdos, aplicações ou serviços, ou à segurança pública), incluindo o direito penal, que imponham, por exemplo, o bloqueio de conteúdos, de aplicações ou de serviços específicos. Além disso, esses prestadores de serviços podem estar sujeitos a medidas conformes com o direito da União, tomadas em execução ou em aplicação de atos legislativos da União ou da legislação nacional, tais como medidas nacionais de aplicação geral, decisões judiciais, decisões de autoridades públicas investidas das competências necessárias ou outras medidas que garantam a conformidade com os atos legislativos da União ou com a legislação nacional (por exemplo, obrigações de cumprimento de decisões judiciais ou ordens das autoridades públicas que imponham o bloqueio de conteúdos ilícitos). A obrigação de conformidade com o direito da União prende-se, entre outros aspetos, com o cumprimento dos requisitos estabelecidos na Carta dos Direitos Fundamentais da União Europeia (a seguir designada «Carta») no que toca às restrições ao exercício dos direitos e liberdades fundamentais. Tal como estabelecido na Diretiva 2002/21/CE do Parlamento Europeu e do Conselho (5), só podem ser aplicadas medidas que restrinjam os direitos ou as liberdades fundamentais se forem adequadas, proporcionadas e necessárias no contexto de uma sociedade democrática, e se a sua execução estiver sujeita a garantias processuais adequadas nos termos da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, incluindo as suas disposições relativas à proteção jurisdicional efetiva e ao processo equitativo.*

## Análise do projeto – IP sem autorização judicial

**PROJETO DE LEI 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.**

### <adicionado com base na 3a versão do relatório CPI Ciber>

Apesar de na terceira versão de seu relatório a CPI dos Cibercrimes ter optado por retirar a proposta de "projeto de lei permitindo que a autoridade de investigação requisite, independentemente de autorização judicial, endereço de IP que identifique conteúdo ou serviço específico, objeto de investigação criminal, mantidos por provedor de conexão ou aplicação de Internet", foi sugerido apoio ao Projeto de Lei do Senado 730, de 2015, de autoria do Senador Otto Alencar, que dispõe sobre investigação criminal e a obtenção de meios de prova de crimes praticados na internet, que em seu art. 2° prevê que "Caso haja indício de prática de crime por intermédio de conexão ou uso de internet, o delegado de polícia ou o membro do Ministério Público, para fins de identificação do responsável pela prática criminosa, poderão requisitar a qualquer provedor de conexão e de aplicações de internet ou administrador de sistema autônomo as informações cadastrais existentes relativas a específico endereço de protocolo de internet", ou seja, ele propõe, assim como fazia a proposta de PL contida nas versões anteriores do relatorio da CPI de Cibercrimes, que as autoridades policiais e o Ministerio Publico possam solicitar a identificação do titular de determinado endereço de IP sem autorização judicial. Por conta disso, ratificamos nosso posicionamento no sentido de que tal medida contraria uma série de direitos fundamentais, conforme demonstraremos a seguir.

Obrigar os provedores de internet a revelar sem prévia autorizaçao judicial os dados do titular do IP que está por trás de cada conexão na internet, além de ser uma afronta ao devido processo legal e o princípio do juiz natural, acaba por estabelecer o perigoso regime de que todos são presumidamente "culpados" na internet brasileira e poderão ser constantemente vigiados pela autoridades de investigação, sem escrutínio judicial prévio. Em outras palavras, seria o fim do princípio do sigilo das comunicações prescrito na Constituição Federal.

Além disso, conforme destacado pelo Comitê Gestor da Internet - CGI.br em sua nota a respeito da CPI dos Cibercrimes: "forçar o entendimento de que o endereço Internet IP seja considerado como dado cadastral para identificação pessoal, mesmo sabendo-se – tal como expressa toda a comunidade técnica global da Internet – que o número IP não é um número fixo que possa ser utilizado para identificação de um usuário (como sucede com números permanentes de registro de um cidadão), posto tratar apenas de um número de localização de uma máquina, na maior parte das vezes dinamicamente atribuído a cada nova conexão" servirá a imputar muitas vezes delitos a pessoas que não os cometeram.

Essa proposta de que o delegado (ou mesmo outras autoridades) possam requerer os dados cadastrais de titulares de IP sem ordem judicial prévia, bastando para isso que "haja indício de prática de crime por intermédio de conexão ou uso de internet," na visão do delegado ou do promotor de justiça, o que os transformaria em verdadeiros juizes. Trata-se de medida atentatória ao próprio Estado Democrático de Direito, na medida em que este se configura especialmente pela distinção de atribuições entre atividades adjudicatórias e atividades de investigação e instrução processual penal. No caso em questão, o delegado passaria a ter a competência para decidir diretamente a respeito da "ilicitude" ou de "elementos de ilicitude" que autorizariam a obtenção imediata do dos dados do titular do endereço de IP, sem a análise prévia de um juiz.

Tal medida viola diretamente a recomendação do Relatório Especial da ONU para Liberdade de Expressão que defende que qualquer determinação dessa natureza deva ser feita por uma autoridade judiciária competente.[191] Além disso, países democráticos como Estados Unidos exigem, naturalmente, a autorização prévia do juiz natural para obtenção dos dados de um titular de número de IP, requerendo a emissão de um "subpoena" ou de um "warrant" conforme o caso. Ambos emitidos por meio do poder judiciário e não por meio da autoridade de investigação ou de instrução processual penal.

Em suma, trata-se de disposição que viola diretamente um grande número de princípios fundamentais, na prática invalidando o sigilo das comunicações, o direito à preservação de intimidade e da vida privada e a privacidade de modo geral.

*19 Relatório do Relator Especial da ONU para Liberdade de Expressão, Frank La Rue, 16 de maio de 2011, par. 75 "Any requests submitted to intermediaries to prevent access to certain content, or to disclose private information for strictly limited purposes such as administration of criminal justice, should be done through an order issued by a court or a competent body which is independent of any political, commercial or other unwarranted influences." Disponível em: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*

**<adicionado com base na 3a versão do relatório CPI Ciber>**

**RECOMENDAÇÃO PARA A CPI DOS CIBERCRIMES:**

Supressão integral da proposta de apoio à discussao do Projeto de Lei do Senado 730, de 2015, de autoria do Senador Otto Alencar, que dispõe sobre investigação criminal e a obtenção de meios de prova de crimes praticados na internet.

**ITS Rio**

Praia do Flamengo, 100 - Cobertura

Rio de Janeiro | CEP 22210-030

(21) 3486-0390 | itsrio@itsrio.org

www.itsrio.org