SOBRE A CPI DE CRIMES CIBERNÉTICOS: ASPECTOS POSITIVOS E NEGATIVOS

E A PARTICIPAÇÃO DA SOCIEDADE CIVIL.

Muito se tem falado sobre a CPI de Crimes Cibernéticos, cujo relatório foi recentemente divulgado. Entretanto, tenho visto algumas posições que são fantasiosas, exageradas ou, ao menos, não totalmente verdadeiras.

Há propostas e projetos de lei que pedem uma maior atenção e discussão da sociedade? Sem dúvida alguma. Estamos correndo o risco de ter decisões injustas? Também é verdade. É possível que os projetos elencados inaugurem uma época de "censura à internet"? De forma alguma. Repito: de forma alguma.

A matéria é extensa, uma vez que o relatório tem mais de 300 páginas e é importante também ler algumas atas das audiências que foram realizadas, de forma que temos aproximadamente 500 páginas de estudo; por este motivo, no texto de hoje farei um pequeno resumo do que pretendo abordar, item por item, nas próximas semanas. Com todo respeito aos colegas que divergem do meu posicionamento, acho importante que não haja apenas uma única narrativa sendo divulgada na internet, e é importante que a sociedade saiba que há profissionais da área que discordam com veemência deste discurso cataclísmico que vem sendo divulgado. A ideia aqui é iniciar um debate, e introduzir vozes dissonantes e até agora pouco ouvidas na conversa – e cumpre dizer que há benefícios para mulheres que estão sendo deixados de lado ou no mínimo sendo encobertos com o conveniente e sedutor disfarce da "liberdade de expressão".

Este texto foi dividido em duas seções: a primeira, um quadro de perguntas e respostas (de forma bem simples) sobre temas que têm tido grande repercussão na mídia.

Na segunda parte do texto, mostrarei os projetos, as indicações, o envio de ofícios e as recomendações, separando os que julgo bons ou importantes dos que requerem atenção – inclusive, tendo em vista o tamanho deste texto, tal método facilita ao leitor localizar os pontos de interesse. Será possível aos leitores verificar que há questões envolvendo fiscalização de empresas quanto ao recolhimento de tributos, melhorias na Lei Maria da Penha e criação de leis específicas para o cyberbullying, para ficar em alguns exemplos.

Nos próximos textos abordarei cada um deles de maneira mais minuciosa. Conto com a colaboração de todos para que o debate seja produtivo.

1. QUESTÕES SUSCITADAS NA MÍDIA

Um dos textos mais veiculados na mídia foi o do ITS-Rio, o qual, com todo respeito, acredito ser um tanto quanto alarmista. Desta forma, ante nossa veemente divergência, cumpre-nos informar ao público o nosso posicionamento, de uma vez que faz-se mister um amplo debate por parte da sociedade quanto aos temas ventilados.

Legenda:

- Não há necessidade de maiores preocupações
- Acompanhar com atenção
- Preocupante – sociedade deve estar atenta

PERGUNTA	RESPOSTA	JUSTIFICATIVA	CUIDADOS
A CPI quer obrigar os provedores de internet a revelarem automaticamente quem está por trás de cada endereço de IP na rede, informando para a polícia o nome, a filiação e o endereço domiciliar da pessoa, sem a necessidade de ordem judicial prévia?	**NÃO**	Hoje, o Marco Civil da internet **já permite que a polícia acesse nome, filiação e endereço de uma pessoa, sem necessidade de ordem judicial.** O que o projeto pleiteia é a inclusão do IP como dado cadastral. **Verificar item 2.3.2 para mais detalhes**.	O problema: não fica claro nos projetos de leis a quais IPs o legislador se refere: seriam todos os IPs utilizados pelo usuário para acessar determinado provedor? Isto seria violação de intimidade? Além disso, como temos IPs dinâmicos, a informação não significaria muito; acessar um site por meio do IP não prova necessariamente nada a não ser que você esteve naquele terminal naquele momento. Por este motivo, creio que este PL mereça uma melhor discussão pela sociedade, até mesmo por questões de eficácia. Juntamente com esta questão deve-se analisar a questão da transformação dos IPs em IPV6 e obrigação de se informar as portas de acesso utilizadas.
A CPI quer transformar as redes sociais em órgãos de censura para proteger a honra de políticos?	**NÃO**	Ela quer um tratamento idêntico para pessoas comuns e gravadoras detentoras de direitos autorais e voltar para o tratamento que a jurisprudência dava ANTES do Marco Civil, tratamento este que foi longamente construído por nossos Tribunais. Políticos hoje já têm como solicitar a retirada de conteúdo; quem sofre são as pessoas comuns, que não dispõem de recursos para contratar advogados. Um exemplo muito bom dos danos que a redação atual do MCI traz é o caso do Leonardo Sakamoto. **Verificar item 2.3.1. para mais detalhes.**	Há na proposta recomendação para retirar conteúdo "igual ou similar" ao que é objeto de solicitação de retirada – este item sim requer atenção, pois pode haver cerceamento à liberdade de expressão. Ver detalhes no item INSERIR.
A CPI pretende estabelecer a censura pura e simples na internet ao criar um novo artigo que permitirá "determinar aos provedores de conexão **bloqueio ao acesso a aplicações de internet por parte dos usuários**"?	**NÃO**	Na verdade, o Marco Civil da internet JÁ PREVÊ bloqueio ao acesso de aplicações em algumas situações, então não há uma inovação. Mesmo que o Marco Civil não previsse tal sanção, o Poder Judiciário possui poderes para determinar tal bloqueio, independentemente do Marco Civil. Não existe apenas o Marco Civil no Brasil – há todo um ordenamento jurídico que deve ser interpretado de forma harmoniosa. **Verificar item 2.4.1. para mais detalhes.**	Não há cuidados a mencionar a não ser o fato de que bloquear acesso a sites criminosos não tem qualquer relação com quebra de neutralidade da rede. Dizer algo semelhante a isso é o mesmo que dizer que a polícia não pode prender um carro que está circulando na rua com pessoas armadas porque isso feriria o direito de ir e vir delas. Como diz Paulo Cândido, "ninguém quer que as operadoras permitam o acesso a pedofilia, mas "devargazinho".
A CPI pretende enviar para a cadeia por 2 anos quem simplesmente violar os "termos de uso" de um site?	**DISCUTÍVEL**	A sugestão de redação do art. 154-A do Código Penal, como está, dá margem a muitas dúvidas – embora a situação colocada pelo ITS nos pareça um tanto quanto catastrófica. **Verificar item 2.2.1. para mais detalhes.**	A sociedade civil deve sim ficar atenta ao prosseguimento deste PL e sugerir alterações, ou ao menos uma melhor definição do tipo penal, para que não haja situações injustas – no entanto, a redação atual também não atende a uma série de situações que precisam ser atendidas.
A CPI quer desviar 10% dos recursos arrecadados pelo Fistel, que têm por objetivo melhorar a	**DISCUTÍVEL**	Com todo respeito, o termo "desviar" soa um tanto quanto exagerado – desviar é praticar um ato ao arrepio da lei. O PL fala	Há uma série de discussões quanto a quais os valores efetivamente arrecadados pelo Fistel, quanto é

qualidade das telecomunicações no Brasil, para financiar a polícia, e isso seria prejudicial para os consumidores?		em destinação de uma parte deste fundo para melhor aparelhar a polícia quanto aos crimes cibernéticos. **Verificar item 2.2.2. para mais detalhes.**	destinado para Anatel e como a Anatel utiliza esta verba, se é que a utiliza inteira. Desta forma, parece precipitado alterar destinação de verba sem que estas questões que vêm sendo ventiladas sejam esclarecidas. Novamente, este ponto merece atenção da sociedade civil; no entanto, é importante ressaltar que aparelhar a polícia para melhorar o combate a crimes cibernéticos não é "colocar a polícia atrás dos meninos que picham sites", ou não só – é também dar à polícia condições de prevenir e reprimir crimes cujos danos patrimoniais e morais podem ser enormes.
A CPI pretende atribuir competência à Polícia Federal para qualquer crime praticado usando um computador ou celular?	**SIM**	No entanto, isto não é realmente uma questão. Tem havido muitas dúvidas e conflitos de competência para decidir o Foro correto, e isto atrasa sobremaneira o andamento dos processos. Vale ler as atas de audiência da CPI sobre o tema para entender melhor a questão. **Verificar item 2.1.15.**	A justificativa do Ministério Público Federal é que as investigações prosseguiriam de forma mais fácil. Não vejo por que agilidade processual poderia ser algo ruim – e realmente, o tão falado "japonês da Federal", como todos sabem, pode ser preso a qualquer momento, não é mesmo?

Como já dito, há sim questões que merecem uma pressão da sociedade civil e temas que merecem ser amadurecidos – mas estamos longe, muito longe, longíssimo, de ter uma legislação como Irã ou Coreia do Norte, com todo o respeito que tenho pelos colegas que pensam o contrário.

E insisto em um ponto: não basta afirmar "este projeto não é bom"; há que se propor alternativas a fim de que os problemas apontados na legislação atual sejam sanados.

2. PROPOSTAS:

2.1. BOAS PROPOSTAS

2.1.1. Alteração da Lei Maria da Penha – PL 5555/2013

O projeto inclui como forma de violência doméstica e familiar contra a mulher a violação da sua intimidade, entendida como "a divulgação, por meio da internet, ou em qualquer outro meio de propagação da informação, sem o seu expresso consentimento, de imagens, informações, dados pessoais, vídeos, áudios, montagens ou fotocomposições da mulher, obtidos no âmbito de relações domésticas, de coabitação ou de hospitalidade".

O projeto também inclui que nos casos em que haja a propagação desta informação "o juiz ordenará ao provedor de serviço de e-mail, perfil de rede social, de hospedagem de site, de hospedagem de blog, de telefonia móvel ou qualquer outro prestador do serviço de propagação de informação, **que remova, no prazo de 24 (vinte e quatro) horas, o conteúdo que viola a intimidade da mulher"**.

Com todo o respeito, não há censura alguma aí – apenas defesa dos interesses de direitos da mulher.

2.1.2. Projeto criando o tipo penal de intimidação sistemática (Bullying) com aumento de pena para casos onde esta intimidação se dê por meio da internet (Cyberbullying) – PL 3686/2015

Todos aqueles que vivem o dia a dia da internet sabem o quão terrível pode se tornar a vida de uma pessoa quando hordas decidem que você não vai ter paz. Não há como ser contra tal projeto, e não há qualquer censura à liberdade de expressão aqui – a menos que se entenda como liberdade de expressão infernizar a vida de um ser humano.

Querem exemplos? Imaginem 50, 100 pessoas passando um dia inteiro se dirigindo a uma pessoa nestes termos:

Para quem não está habituado, é importante informar que isto acontece TODO DIA na internet.

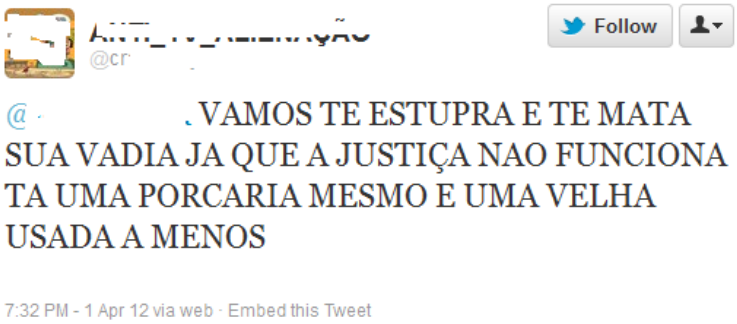
2.1.3. Projeto criando o tipo penal de Incitação Virtual ao Crime – PL 7544/2014

O direito penal utiliza-se do que em Direito é chamado de "tipo fechado", ou seja, grosso modo, não é possível interpretar de forma ampliativa o que está descrito como crime, pois isto poderia prejudicar o réu. Desta forma, como há uma discussão sobre o fato de incitação ao crime por meio de internet configurar incitação ao crime, é salutar que haja este cuidado.

CÓDIGO PENAL ATUAL	SUGESTÃO DE REDAÇÃO PELA CPI
Incitação ao crime Art. 286 - Incitar, publicamente, a prática de crime: Pena - detenção, de três a seis meses, ou multa.	**"Incitação Virtual ao Crime** Art. 286-A - Publicar, por meio de rede social ou de qualquer veículo de comunicação virtual, conteúdo que incite a prática de crime ou de violência à pessoa: Pena - detenção, de 3 (três) a 6 (seis) meses e multa. § 1º - Se da veiculação de conteúdo a que se refere o caput deste artigo, resultar lesão corporal ou a morte da pessoa exposta ou de terceiros, o

	autor da divulgação responderá, concorrentemente com o agente, pelos crimes previstos nos artigos 121 e 129, deste Código Penal, conforme o caso. § 2º - A pena é agravada em 1/3 se a publicação tiver sido veiculada por perfil apócrifo.”

Para quem não sabe como funcionam as redes sociais, seguem exemplos:



Cumpre lembrar que há várias prisões efetuadas entendendo como aplicável o crime de incitação ao crime quando este é cometido pela internet, mesmo sem haver a inclusão sugerida pela CPI.

Dois são presos por incitar crimes de ódio e intolerância pela internet

SOLANGE SPIGLIATTI

22 Março 2012 | 09h 21 - Atualizado: 22 Março 2012 | 10h 51

Criminosos também fizeram referência de apoio ao atirador da escola de Realengo

São Paulo, 22 - Duas pessoas foram presas nesta quinta-feira, 22, acusadas usarem a internet para espalhar mensagens de apologia de crimes graves e da violência, principalmente contra mulheres, negros, homossexuais, nordestinos e judeus, além da incitação do abuso sexual de menores, segundo a Polícia Federal.

A Operação Intolerância prendeu Emerson Eduardo Rodrigues e Marcelo Valle Silveira Mello, moradores de Curitiba e Brasília, respectivamente. Eles foram presos preventivamente por supostamente serem os responsáveis pelo site silviokoerick.org.

2.1.4. Inclusão de crimes decorrentes de pedofilia como crime hediondo – PL 1776/15

O texto do PL está escrito de forma muito precária, uma vez que pedofilia em si não é crime, e sim a prática de atos que decorram da pedofilia. Entretanto, genericamente e de forma não técnica, tornou-se popular a associação de pedofilia com crimes sexuais praticados em que as vítimas sejam menores de idade.

Feita esta ressalva, além do fato de que quando se tem muitos crimes hediondos eles deixam de sê-lo, não há nada de anormal nesta proposta.

Também é importante ressalvar que o PL em questão não alude à prática de crimes de natureza sexual na internet – motivo pelo qual não se compreende sua inclusão no rol de sugestões dentro de uma CPI visando entender os crimes cibernéticos.

2.1.5. Divulgação indevida de dados pessoais na internet – PL 1755/2015

Também aqui, não vejo motivo pelo qual tal iniciativa poderia configurar censura. Aqueles que acham correto o exercício da autotutela certamente correrão riscos, mas salvo engano, de há muito a sociedade civil resolveu que autotutela não faz parte de nosso contrato social.

2.1.6. Inclusão de artigo no Marco Civil de modo a melhor enquadrar as filiais nacionais de empresas estrangeiras do setor – pág. 165 do Relatório

ART. 12 DO MARCO CIVIL	SUGESTÃO DE REDAÇÃO PELA CPI – ART. 22
Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11. Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.	"Art. 22- Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. § 2o No caso em que as operações de que trata o artigo 11 sejam realizadas no exterior, desde que o serviço seja ofertado ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil, responde solidariamente pelo fornecimento sua filial, sucursal, escritório ou estabelecimento situado no País."

O Marco Civil da internet já prevê que, no caso de sanções que devam ser impostas às empresas no caso de algumas infrações (lembrando que o rol de sanções aplicáveis às empresas não é exaustivo, tampouco o Marco Civil o único diploma legal vigente

no nosso ordenamento jurídico), responde solidariamente por tais sanções a filial, a sucursal ou estabelecimento situado no País.

No entanto, não há um artigo dispondo especificamente que empresas que possuam filiais, sucursais, estabelecimento no País, ou mesmo do próprio grupo econômico, devam atender a quaisquer ordens judiciais.

Na verdade, utilizando as regras mais comezinhas de interpretação jurídica esta questão é facilmente solucionada, uma vez que a jurisprudência e a doutrina empregam de há muito a chamada "teoria da aparência", ou "desconsideração da personalidade jurídica" (isto foi tratado neste texto), bem como o princípio da economia processual (não há motivo para utilizar um tratado de cooperação internacional quando podemos fazer uma solicitação aos escritórios da empresa que se encontram em território nacional).

Entretanto, como atualmente vivemos em um mundo onde regras de interpretação jurídica são pouco utilizadas, onde se atropelam princípios elementares de direito e onde por vezes parece prevalever a literalidade da lei, lei esta vista isoladamente, sem análise de todo ordenamento jurídico, é justo que deixe o óbvio ainda mais óbvio, motivo pelo qual não vejo qualquer óbice ao PL, a não ser a sua obviedade.

2.1.7. Envio de ofícios aos Poderes Executivos do Estado e do Município de São Paulo e Ministério Público do Estado de São Paulo, recomendando que se investigue eventual irregularidade na falta de recolhimento de tributos, bem como prática, em tese, de crime contra a ordem tributária previsto na Lei 8.137/90) – pág. 246 do Relatório e seguintes

Certamente por falta de espaço não houve maiores manifestações sobre o fato de que a CPI solicita que o Município, o Estado e o Ministério Público de São Paulo **investiguem empresas como Facebook, Google, Twitter e similares** em razão do não-recolhimento de tributos. Por óbvio, ninguém pode achar abusiva ou censora uma medida como esta, certo?

> Constatou-se, todavia, que a Prefeitura Municipal informou à empresa Facebook Serviços Online do Brasil Ltda. por meio da Solução de Consulta nº 42/2013 que a mesma está sujeita ao recolhimento do tributo com base em receitas de intermediação de serviços, situação essa que também pode ocorrer em relação às outras duas empresas.
>
> Esta Solução de Consulta não foi mencionada pela empresa a esta CPI, o que pode ter ocorrido com o intuito de ocultar irregularidade na falta do recolhimento do tributo, situação que, em tese, pode caracterizar a prática de crime contra a ordem tributária (Lei nº 8.137, de 27 de dezembro de 1990).

Cumpre esclarecer que a autora em nenhum momento está acusando quaisquer empresas de não estarem cumprindo com suas obrigações tributárias – apenas afirma que o pedido de investigação consta do relatório da CPI e que houve pouca ou nenhuma divulgação quanto a este fato.

2.1.8. Projeto de Lei que adiciona a educação digital entre as diretrizes do Plano Nacional de Educação – PNE – pág. 211 do Relatório e seguintes

Alguém tem algum argumento contra esta indicação? Eu não tenho.

2.1.9. Propõe que a Comissão de Ciência e Tecnologia, Comunicação e Informática fiscalize, com o 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. 214 do Relatório e seguintes

A lei existente (repita-se, lei JÁ EM VIGOR) requer que a aquisição de telefones pré-pagos seja feita mediante identificação do seu comprador. Segundo análise da CPI, este controle de cadastro não está sendo feito. Não se trata, mais uma vez, de "censura", ou de "controle da internet", e sim de uma proposta para que a Anatel cumpra a sua função. Alguém tem algo contra agências reguladoras cumprirem suas funções?

2.1.10. Propõe que a Comissão de Ciência Propõe que a Comissão de Ciência e Tecnologia, Comunicação e Informática fiscalize, com o auxílio do Tribunal de Contas da União – TCU, as ações de acompanhamento e controle da Agência Nacional de Telecomunicações – Anatel, acerca da correta bilhetagem dos serviços de dados por parte das prestadoras do serviço móvel pessoal – pág. 218 do Relatório e seguintes

Novamente, temos um caso no qual a CPI pede maior fiscalização, por parte da Anatel, quanto à cobrança de uso de dados pelas empresas responsáveis por tal prestação de serviço. Não há aqui qualquer irregularidade – a não ser estarmos em uma curiosa situação onde uma agência reguladora é instada a cumprir com suas funções.

2.1.11. Indicação ao Poder Executivo, sugerindo a adoção de medidas para melhorar a segurança da infraestrutura de Tecnologia da Informação da Administração Pública e outras providências

Há questões técnicas a ser analisadas quanto à possibilidade de tal indicação, mas não há qualquer ilicitude ou abuso por parte da CPI neste item.

2.1.12. Indicação ao CNJ sugerindo a criação de varas judiciais especializadas em crimes eletrônicos – pág. 237 do Relatório e seguintes.

Os profissionais que militam na área sabem quão complexo é fazer com que os magistrados entendam algumas questões envolvendo o direito digital. Vejo tal medida como benéfica.

2.1.13. Criação de um Código de Boas Práticas a ser adotado pelas entidades envolvidas com a publicidade no meio digital, para evitar a comercialização de espaço para anúncios publicitários em plataformas digitais que disponibilizem conteúdos ilícitos, pratiquem condutas ilegais e/ou fomentem a prática de tais condutas pelos seus usuários – pág. 120 do Relatório

Não há qualquer ilegalidade ou infração a princípios constitucionais nesta medida; resta saber se há viabilidade técnica para que tal Código seja eficaz.

2.1.14. Perda dos instrumentos do crime doloso como efeito da condenação – sugestão de PL constante da pág. 181 do Relatório

Não me parece que haja algo grave nesta questão proposta, mas gostaria de ouvir os colegas a respeito.

TEXTO DO CÓDIGO PENAL EM VIGOR	SUGESTÃO DE REDAÇÃO PELA CPI
Art. 91 Art. 91 - São efeitos da condenação: ... II - a perda em favor da União, ressalvado o direito do lesado ou de terceiro de boa-fé: a) dos instrumentos do crime, desde que consistam em coisas cujo fabrico, alienação, uso, porte ou detenção constitua fato ilícito;	"Art. 91 Art. 91 - São efeitos da condenação: ... II - a perda em favor da União, ressalvado o direito do lesado ou de terceiro de boa-fé: a) dos instrumentos do crime doloso, em qualquer hipótese, e dos instrumentos do crime culposo, desde que consistam em coisas cujo fabrico, alienação, uso, porte ou detenção constitua fato ilícito;"

2.1.15. Projeto de Lei que inclui os crimes praticados contra ou mediante computador, conectado ou não à rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme – pág. 194 Relatório e seguintes

Com todo o respeito para com os colegas que divergem quanto a este tema, a justificativa para o PL me convenceu:

JUSTIFICAÇÃO

Conforme apurado por esta Comissão Parlamentar de Inquérito, a legislação brasileira ainda é muito incipiente no que diz respeito aos crimes cibernéticos.

Uma questão que chamou a atenção, por exemplo, diz respeito à ausência de uma norma específica no que tange à competência para a investigação desses delitos. Assim, os casos envolvendo crimes praticados na internet – que geralmente possuem repercussão interestadual ou, até mesmo, internacional – continuam sendo, na maioria das vezes, de competência investigativa das policias civis estaduais.

Entendemos, porém, que esses delitos, quando necessitarem de uma repressão uniforme, devem ficar a cargo da Polícia Federal sempre que houver repercussão interestadual ou internacional.

Há enormes questões de conflitos de competência quando falamos de internet – e as recentes reviravoltas na Operação Lava Jato mostram o quanto tais conflitos de competência podem ser perniciosos e alongar o processo. Basta dizer que enquanto o conflito de competência não é solucionado, a questão central, o mérito do processo, não é discutida. Acho importante para acelerar o provimento jurisdicional que, como é sabido, não basta ser dado, mas deve ser dado a tempo de reparar o dano causado.

Assim sendo, não vejo esta questão como um grande problema.

2.2. PROPOSTAS QUE NECESSITAM DE MUITA ATENÇÃO

2.2.1. Alteração da Lei Carolina Dieckmann

Para quem não sabe, por uma destas ironias do destino, a Lei conhecida como Lei Carolina Dieckmann, criada em razão do vazamento de fotos íntimas da atriz, não pode ser aplicada ao seu caso. Com base neste fato, a CPI recomendou nova redação ao artigo 154-A do Código Penal.

REDAÇÃO ATUAL	SUGESTÃO DE REDAÇÃO PELA CPI
	"**Acesso indevido a sistema informatizado**
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:**	Art. 154-A. **Acessar, indevidamente e por qualquer meio, sistema informatizado, ou nele permanecer contra a vontade expressa ou tácita de quem de direito:**
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa	**Pena - detenção, de seis meses a dois anos, e multa.**
§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.	§ 1º Na mesma pena incorre quem, sem autorização ou indevidamente, produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta descrita no *caput*.
§ 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.	§ 2º Se do acesso resultar: I - prejuízo econômico;

§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave § 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. § 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal	II - destruição, danificação, inutilização, adulteração ou supressão de dados informatizados, ainda que parcialmente; III - instalação de vulnerabilidade informática no dispositivo acessado; IV - obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, arquivos, senhas, informações ou outros documentos ou dados privados; V - controle remoto não autorizado do dispositivo acessado: Pena - reclusão, de um a quatro anos, e multa, se a conduta não constitui crime mais grave. § 3º Se o crime é cometido contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal; V - a Administração Pública direta ou indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos: Pena - reclusão, de dois a quatro anos, e multa. § 4º Nas hipóteses dos §§ 2º e 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados, arquivos, senhas ou informações obtidas, ou se o acesso se dá mediante violação de mecanismo de segurança. § 5º Para os fins deste artigo, considera-se: I - 'sistema informatizado': o computador ou qualquer dispositivo ou conjunto de dispositivos, interligados ou associados, em que um ou mais de um entre eles desenvolve o tratamento automatizado de dados informatizados através da execução de programas de computador, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informatizados armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos; II - 'dados informatizados': qualquer representação de fatos, informações ou conceitos sob a forma suscetível de processamento em um sistema informatizado, incluindo programas de computador; III - 'mecanismo de segurança': qualquer mecanismo que tem como finalidade evitar o acesso de terceiro não legítimo a um sistema informatizado e garantir autenticidade do detentor legítimo de acesso."

A diferença entre uma redação e outra é clara: na atual, usa-se a expressão "**invadir dispositivo**", enquanto que a sugestão de redação da CPI menciona **"acessar indevidamente sistema informatizado".** É esta sugestão uma das mais criticadas, pois, segundo alguns juristas, com esta redação, "infringir termos de uso" de um site poderia ser considerado crime.

Não se pode negar que, em tempos em que pessoas portando vinagre na rua estão presas, há que se ter um extremo cuidado na redação de leis – e, evidentemente, todo cuidado é pouco. A intenção do legislador, embora não se aplique quando da análise de caso concreto, é justamente coibir danos como os causados à atriz Carolina Dieckmann. Ora, de uma vez que os profissionais da área vislumbram possibilidade de excessos, é necessário que a redação deste tipo legal seja mais bem burilada, enfim, seja mais bem discutida pela sociedade. Para isto, é importante estarmos atentos ao processo legislativo, que ainda está em sua fase inicial. Discutir redação de dispositivo legal é rotina do processo legislativo, e deveria ser rotina a sociedade civil acompanhá-lo – mas críticas, discussões e acompanhamento são muito distintos de simplesmente afirmar "com a aprovação desta lei, o japonês da Federal irá à sua casa caso você descumpra os termos do Facebook". Hipérboles são sempre más conselheiras quando estamos tentando dar maior tecnicidade a um texto legal.

Desta forma, sim, esta sugestão da CPI merece atenção e discussão da sociedade civil – o que é diferente de acreditarmos que entraremos em breve em um estado de vigilância.

2.2.2. Projeto de Lei visando à alteração da Lei 5070/66 para autorizar uso dos recursos do Fistel por órgãos da Polícia Judiciária

Projeto cujo posicionamento é complexo.

O **Fundo de Fiscalização das Telecomunicações** (Fistel) é um fundo contábil, formado pela arrecadação da Taxa de Fiscalização de Instalação (TFI) e da Taxa de Fiscalização de Funcionamento (TFF), cobradas pela Agência Nacional de Telecomunicações (Anatel), sendo os recursos arrecadados uma das fontes de recursos da Anatel.

À primeira vista, não é ruim que a Polícia Judiciária tenha mais recursos para cumprir o seu papel; no entanto, fazendo uma rápida pesquisa, percebe-se que o Fistel tem suspeitas de desvio de fundos, ou ao menos divergências sérias de valores arrecadados, causando uma situação delicada entre o Fistel e a Anatel. Há também recomendações sérias feitas pelo Ministério Público Federal a respeito do tema.

Tendo isto em conta, não sabemos se autorizar o uso dos recursos para outros fins que não os originariamente destinados seria uma proposta interessante.

2.3. PROPOSTAS QUE REQUEREM ALGUMA ATENÇÃO

2.3.1. Projeto de lei dispondo sobre procedimento específico para a retirada de conteúdos que atentem contra a honra

REDAÇÃO ATUAL DO MARCO CIVIL	SUGESTÃO DE REDAÇÃO PELA CPI
Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros. **Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.** **§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.** **§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.** § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial,	**"Art. 21-A. Ao provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros, identificados ou não, poderá caber responsabilização subsidiária por prejuízos decorrentes da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais que atentem contra a honra de maneira acintosa quando, após o recebimento de notificação pelo participante, vítima ou objeto ou seu representante legal, deixar de promover, dentro do prazo de 48 (quarenta e oito) horas, no âmbito do seu serviço, a indisponibilização desse conteúdo.** **§ 1º A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado e a verificação da legitimidade para apresentação do pedido.** **Art. 21-B Os provedores de aplicação deverão tomar as providências técnicas, nos limites de suas aplicações, para assegurar que o conteúdo infringente, objeto da ordem judicial de que trata esta Seção, continue indisponível em caso de cópia ou conteúdo relacionado, dispensada a necessidade de nova ordem judicial ou notificação para a retirada desses novos materiais.** Parágrafo único. Para os efeitos deste artigo, são consideradas: I – cópia: aquele conteúdo idêntico ao original ou similar que contenha parte do conteúdo original e que continue a configurar a característica considerada como infringente;

existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação. Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário. Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização. **Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.** **Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.**	II – conteúdo relacionado: aquele que faz referência ao fato considerado como infringente.”

Este é o projeto de lei que alguns juristas entendem beneficiar políticos influentes e trazer “censura e vedação à liberdade de expressão”.

Cumpre, antes de entrarmos na proposta feita pela CPI, relatar alguns fatos. Até a edição do Marco Civil da internet, construiu-se uma jurisprudência (ou seja, definiu-se uma linha segura de decisões) no sentido de que o provedor de aplicações não tinha obrigação de adivinhar que este ou aquele conteúdo seria danoso a uma pessoa e portanto, não teria a obrigação de retirá-lo sem que alguém o solicitasse. Entretanto, a partir do momento em que o provedor tivesse conhecimento de que aquele conteúdo seria danoso, ou retiraria o conteúdo ou responsabilizar-se-ia pelos danos causados a partir de então. Houve um julgamento considerado leading case, relatado pela Ministra do STJ Nancy Andrighi exatamente neste sentido, e destaco da matéria acima mencionada:

> Mesmo que fosse possível vigiar a conduta dos usuários sem descaracterizar o serviço prestado pelo provedor, haveria de se considerar outro problema: os critérios que autorizariam o veto ou o descarte de determinada informação. Para a ministra, seria impossível delimitar parâmetros de que pudessem se valer os provedores para definir se uma mensagem ou imagem é

potencialmente ofensiva. "Entretanto, também não é razoável deixar a sociedade desamparada frente à prática, cada vez mais corriqueira, de se utilizar comunidades virtuais como artifício para a consecução de atividades ilegais", declarou em seu voto.

Ao negar provimento ao recurso, a ministra destacou que os provedores de conteúdo não respondem objetivamente pela inserção no site, por terceiros, de informações ilegais e que eles não podem ser obrigados a exercer um controle prévio do conteúdo das informações postadas no site por seus usuários. Mas devem, assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos, mantendo, dessa forma, um sistema minimamente eficaz de identificação de seus usuários.

Ou seja, a jurisprudência havia chegado em um ponto bastante razoável: o provedor não tem a obrigação de adivinhar se um conteúdo é danoso ou não e decidir retirá-lo ou não; mas a partir do momento em que tem ciência daquele conteúdo, deve sim responsabilizar-se pela manutenção do conteúdo em seu site, pois isto decorre do risco do seu negócio.

Há que se pensar no equilíbrio entre os princípios jurídicos: a liberdade de expressão, ainda que ampla, tem alguns limites, limites estes inclusive que dependem da personalidade ou dos fatos sobre os quais esta manifestação se dá. Assim, grosso modo, uma pessoa pouco conhecida tem maior direito à intimidade do que uma autoridade.

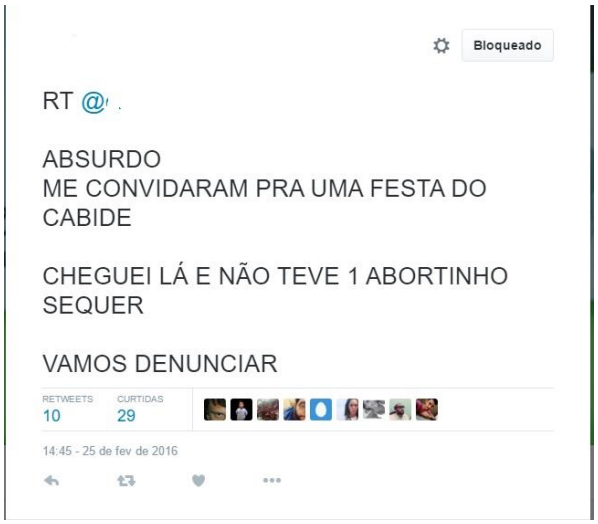
Pois bem, o que ocorreu com a edição do Marco Civil? Criou-se um artigo “Revolução dos Bichos” sobre retirada de conteúdo, em que:

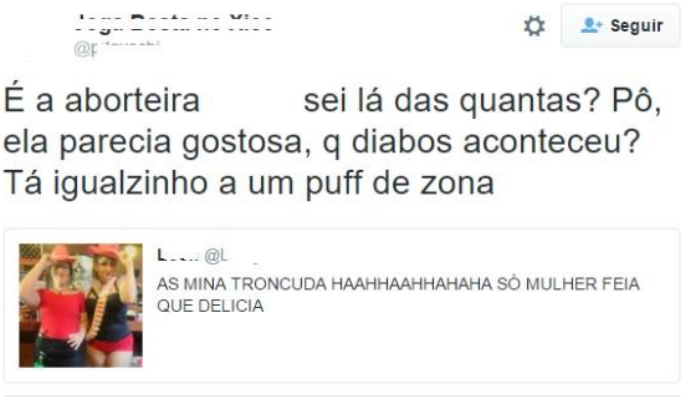
- conteúdos que contivessem infração a direitos autorais (leia-se “gravadoras”) seriam removidos imediatamente após notificação, sob pena de responsabilidade subsidiária (ou seja, seriam também responsáveis pelo dano);

- conteúdos que contivessem nudez ou atos sexuais seriam removidos imediatamente após notificação, sob pena de responsabilidade subsidiária;

- outros conteúdos difamatórios somente poderiam ser retirados após ordem judicial que assim o determinasse.

Realmente, à primeira vista, até parece bastante justo, a não ser pelo fato de que o dia a dia da internet é feito de ofensas gratuitas, de hordas de pessoas ofendendo uma vítima por vezes escolhida a dedo, vítima esta que nem sempre tem recursos para ir ao Judiciário. Além disso, temos o fator tempo: 24h na internet é uma vida. Uma liminar para retirada de conteúdo demora, no mínimo, uns 10 dias para ser obtida. Neste intervalo de tempo, a vítima está lá, exposta, sendo achincalhada. Para se ter uma ideia do nível de constrangimento a que alguém pode ser exposto na internet, vejamos aqui um exemplo (o nome da vítima e o do ofensor foram ocultados).





Os provedores de aplicação não são gratuitos; eles recebem, em troca da utilização de sua plataforma, nossas informações. Eles têm um NEGÓCIO. É justo que se responsabilizem pelos danos que o seu negócio possa causar a alguém a partir do momento em que têm ciência de que podem estar causando danos a terceiros.

O argumento da censura aqui não se sustenta. A uma, porque o provedor não é obrigado a retirar o conteúdo, ele apenas passa a ser solidariamente responsável e tem condições de arcar com isso; a duas, porque não há como se comparar ofensas a pessoas comuns a textos sobre personalidades – e mesmo estes devem ser feitos com o que o Direito chama de "*jus narrandi*", ou seja, com a intenção de narrar os fatos e não de ofender. A Constituição Brasileira delimita a liberdade de expressão.

Outro ponto importante: NÃO É VERDADE que esta alteração traria censura em razão de má interpretação dos juízes. Em primeiro lugar, porque não podemos pensar em uma legislação sob o ponto de vista do seu desvirtuamento, e sim cobrar sua aplicação de forma correta; em segundo lugar, porque HOJE, COM O MARCO CIVIL EM VIGOR, A MÁ APLICAÇÃO DA LEI JÁ EXISTE.

Não estamos falando, portanto, de uma inovação visando cercear liberdade de expressão: estamos falando de uma jurisprudência longamente construída no curso dos anos que foi INTERROMPIDA ARTIFICIALMENTE pelo Marco Civil, mantendo, no entanto, privilégios para grandes gravadoras e detentores de direitos autorais, enquanto pessoas comuns sofrem no dia a dia da internet.

Lembre-se ainda que, mesmo com a responsabilidade sendo reconhecida após a ordem judicial, os provedores de aplicação NÃO CUMPREM ORDENS JUDICIAIS, como é sabido. Podem continuar não cumprindo quando entenderem tratar-se de caso de defesa de liberdade de expressão, ou podem ser razoáveis e analisar a retirada de conteúdo quando uma pessoa comum está sendo vítima de ofensas.

Há, porém, uma crítica a ser feita neste projeto de lei elaborado pela CPI: a obrigação de se retirar também "conteúdo relacionado" ao tema considerado ofensivo. Aí sim, temos um juízo de valor que não cabe ao provedor de aplicação fazer – cumpre, no entanto, deixar claro que devem ser criadas formas de cumprimento eficaz das determinações judiciais que, ressalte-se, também não são cumpridas.

2.3.2. Projeto de Lei Alterando a Lei das Organizações Criminosas, a Lei da Lavagem de Dinheiro e o Marco Civil da Internet para incluir no rol das informações cadastrais de usuário o endereço IP – pág. 145 do Relatório e seguintes, bem como PL 3237/15.

A CPI tem como um de seus objetivos incluir o IP no rol de dados cadastrais, o que é tema bastante discutível. Vejamos os argumentos constantes do relatório:

> Durante as oitivas verificamos que as autoridades de investigação muitas vezes não possuem acesso a diversas informações dos perpetuadores de crimes devido a facilidades da própria tecnologia – como mecanismos de ocultamento de IPs – mas também pela simples falta de coleta ou acesso a dados essenciais do internauta.
>
> O estudo aprofundado do assunto nos permite concluir que a guarda do endereço IP no momento de criação das contas possibilitaria às autoridades de investigação, encontrar mais facilmente autores de eventuais ofensas criminais. Ademais, a equiparação do endereço IP do usuário de internet a dado cadastral infligiria maior celeridade ao processo investigativo.
>
> Mediante a sistemática atual, em caso de processo de investigação em andamento, a autoridade judicial possui acesso aos dados cadastrais de qualquer usuário da telefonia. No entanto, para se obter o usuário que se encontra por trás de determinado endereço IP é necessário recorrer a mandato judicial e realizar o processo de quebra em três etapas. Primeiro junto ao aplicativo, segundo, junto à autoridade de registro da internet e, terceiro, junto à operadora de telefonia. Diversas autoridades indicaram a demora desses processos por diversos motivos. Desde a recusa no atendimento a solicitações por parte de empresas de internet que possuem suas bases de dados no exterior, até a falta de disponibilidade de juízes de plantão para emissão de ordens judiciais que autorizem a quebra do sigilo nas diversas etapas.
>
> Nesse contexto, se o endereço IP fosse tratado como dado cadastral, as autoridades de investigação poderiam ter acesso imediato ao individuo pessoa física, na maioria dos casos. A empresa responsável pela aplicação de internet (e pelos logs de navegação, de acordo com o Marco Civil da Internet) teria que informar o endereço IP, assim como a operadora de conexão à internet. O cruzamento imediato dessas informações permitiria a identificação de internautas investigados de maneira automática e imediata. Gostaríamos de ressaltar neste ponto do relatório que a equiparação que ora propomos não implica em franquear o acesso de policiais aos dados de qualquer internauta. Nossa proposta não altera a sistemática atual já prevista
>
> Assim, como forma de aumentar a eficácia das investigações, propomos **Projeto de Lei alterando a Lei das Organizações Criminosas, a Lei da Lavagem de Dinheiro e o Marco Civil da Internet para incluir no rol das informações cadastrais de usuários o endereço IP.** (Parte III, 1.6)

Este projeto causa espécie. IP não está associado a uma pessoa específica, mas sim a um terminal. No entanto, o MCI (art. 5º, III) denomina como IP o "endereço de protocolo de internet", afirmando ainda que este seria "o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais".

Ora, o próprio MCI já permite que o endereço físico do usuário seja fornecido à autoridade policial sem que haja necessidade de uma ordem judicial. Poderíamos, partindo desta premissa, inferir que, se o endereço físico é acessível sem ordem judicial, o endereço de acesso daquele usuário também pode ser considerado dado cadastral?

Responderia que eu até entendo que sim, afinal, ambos são "endereço", e não vejo nenhuma invasão de privacidade aí.

No entanto, a questão dos IPs dinâmicos faz com que essa conclusão não só reste inócua como também possa vir a causar problemas sérios ou, na melhor das hipóteses, não ajude a solucionar nenhuma investigação. Qual a serventia de termos a

associação de uma pessoa a uma máquina determinada, que pode, inclusive, em função do uso de IPs dinâmicos, nem mesmo ser aquela máquina?

Em nota sobre a CPI dos Crimes Cibernéticos, a CGI.br afirma 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".

Temos ainda um outro ponto crítico: a quais IPs as autoridades poderão ter acesso? A todos os registros de acesso cadastrados? Entendo que isso viole a privacidade e necessite de ordem judicial (e o problema aí não é o tempo que se perde solicitando referida ordem, mas o fato de que algumas empresas DESCUMPREM ordens judiciais tendo inclusive o respaldo da população, iludida com o manto da "liberdade de expressão").

ART. 10 DO MARCO CIVIL	SUGESTÃO DE REDAÇÃO PELA CPI
Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. **§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.** § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. **§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.**	"Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. **§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.** § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. § 3º O disposto no **caput** não impede o acesso aos dados cadastrais de investigado que informem qualificação pessoal, filiação, endereço **e endereço IP**, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição."

ART. 15 Lei 12.850	SUGESTÃO DE REDAÇÃO PELA CPI
Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos **pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito.**	"Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente **a qualificação pessoal, a filiação, o endereço e o endereço IP mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito. "**

Na proposta acima, a intenção fica mais clara: pretende-se que a autoridade acesse o IP mantido pela Justiça Eleitoral

ART. 17 B da Lei 9613/98	SUGESTÃO DE REDAÇÃO PELA CPI
Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas	"Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação, endereço **e endereço IP**, independentemente de autorização judicial, mantidos pela Justiça

telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.	Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito."

É importante ressaltar que a discussão do que seja ou não dado pessoal está presente também na regulamentação do MCI, de uma vez que não temos hoje tal definição.

Assim, para concluir: os textos merecem melhor definição, sob pena de a autoridade judicial ter acesso a todos os IPs utilizados por um usuário – e isso seria sim violação à privacidade. Além disso, na hipótese de ser informado apenas um acesso, corre-se o risco de a informação restar inútil à autoridade investigadora.

2.3.3. – Indicação à Agência Nacional de Telecomunicações, sugerindo a adoção das medidas necessárias para a implantação do IPV6 no país – pág. 148 do Relatório e seguintes

Uma das propostas para solucionar a questão do item acima (a impossibilidade de se identificar o usuário pelo número de seu IP, de uma vez que este é não só associado a uma máquina, como também há atribuição de outros números a cada nova conexão) seria a de implantar o quanto antes o chamado IPV6 no País.

Vejamos a justificativa do relatório:

> Em diversas audiências públicas os membros desta CPI foram alertados de que novas modalidades de conexão à internet se utilizam de tecnologias que permitem o compartilhamento de endereços IPs, isto é, compartilham o mesmo número que identificaria de maneira única o dispositivo conectado à internet, o que impediria a correta identificação dos internautas. Nesse sentido, o Serviço de Repressão a Crimes Cibernéticos da Polícia Federal salienta a necessidade da guarda não apenas dos endereços IPs, mas também das portas utilizadas por cada usuário[28].
>
> No entanto, devido ao atual estágio de desenvolvimento e outras limitações, tais como de adaptação de conteúdos e de equipamentos, como relatado por especialistas e operadoras de telecomunicações em Audiência Pública nesta CPI, não é possível tecnicamente a adoção imediata da nova versão. Todavia, entendemos que a Anatel não tem tratado a questão da migração para o IPv6 com a prioridade necessária. Entendemos que a agência deveria incentivar mais enfaticamente a sua adoção por parte da indústria e das empresas do setor.
>
> No aprofundamento da análise do tema, esta Sub-Relatoria pondera que a falha na identificação dos internautas não decorre naturalmente do uso da tecnologia e sim, de falha na regulamentação.

Notadamente, a definição, pelo Marco Civil da Internet (MCI, Lei nº 12.965/14), do que constitua provedor de internet e suas obrigações deixa um vazio legal para determinados tipos de provedores de conexão. O MCI dispõe que apenas os administradores que possuem endereços IP diretamente alocados pela autoridade de registro da internet no Brasil, o Cgi.br, possuem a necessidade de guardar registros de conexão de seus usuários. Para esclarecimento, chamaremos esses provedores de primários. Normalmente provedores primários são grandes empresas e entidades governamentais, que gerenciam grande quantidade de usuários e de conexões. Dentre elas, as companhias telefônicas, do cabo e entidades Estaduais e Federais.

Assim, de acordo com a Lei, provedores de conexão não primários, que por sua vez são usuários daqueles provedores, estão isentos da obrigação da guarda de registros de usuários. Como consequência, indivíduos podem acometer toda sorte de crimes cibernéticos quando conectados a esses provedores não primários com a certeza da impunidade, uma vez que seus registros de conexão não serão guardados.

De maneira acertada, e afortunada para esta CPI, essa incorreção no MCI já foi objeto de proposição, na forma do PL 3.237/15. Por esses motivos, concluímos por:

1. **manifestar nosso apoio ao PL 3.237/15 que determina a guarda unívoca dos registros de conexão por todos os provedores de conexão;** (Parte III, 5) **e**
2. **oferecer Indicação ao Sr. Ministro de Estado das Comunicações sugerindo à Agência Nacional de Telecomunicações a adoção das medidas necessárias para a implantação do IPV6 no país**. (Parte III, 3.5)

ART. 5º DO MARCO CIVIL	SUGESTÃO DE REDAÇÃO PELA CPI
Art. 5º Para os efeitos desta Lei, considera-se: I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes; II - terminal: o computador ou qualquer dispositivo que se conecte à internet; III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;	

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País; V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP; VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados; VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.	"IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País **ou que preste serviço de conexão à internet mediante contratação remunerada, ou, ainda, disponível gratuitamente ao público em geral;"** "§ 7o Administrador de sistema autônomo que preste serviço de conexão à internet disponível gratuitamente ao público em geral deverá manter cadastro atualizado dos seus usuários, de modo a permitir a disponibilização dos registros de que trata o § 1o , do art. 10 na forma prescrita por aquele dispositivo." (NR) Art. 3º Esta lei entra em vigor na data da sua publicação

ART. 13 º DO MARCO CIVIL	**SUGESTÃO DE REDAÇÃO PELA CPI**
Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.	"Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento." **"§ 7o Administrador de sistema autônomo que preste serviço de conexão à internet disponível gratuitamente ao público em geral deverá manter cadastro atualizado dos seus usuários, de modo a permitir a disponibilização dos registros de que trata o § 1o , do art. 10 na forma prescrita por aquele dispositivo."**

Estudando o tema, encontrei texto de Fabio Nori (in *Direito & Internet III*, Tomo II, pág, 169 e seguintes), que merece citação:

o tráfego p...

Não se espera o fim do *uso* do IPv4 senão em mais de uma década, já que o acesso a uma página, ou aplicação, usando IPv6 depende de uma série de fatores alheios à vontade do usuário ou mesmo dos provedores de conexão ou de aplicações. Os equipamentos dos usuários e o conteúdo da aplicação afetam diretamente essa estatística e tornam lenta a migração desse tráfego.

Essa conformação do mercado com o esgotamento dos endereços IPv4, associada à pouca quantidade de equipamentos e sítios compatíveis com o IPv6, faz com que os acessos dos usuários à internet serão feitos através de endereços IP *compartilhados*. Nessa condição, diversos usuários usarão um único endereço IP.

A informação do IP e da data e da hora da conexão prevista na definição de registro de conexão não será mais suficiente para identificar *univocamente* um terminal, ou pessoa, sendo necessário algum procedimento ou informação complementar para permitir essa identificação. A informação da *porta*[18] usada no acesso à aplicação, coletada tanto no registro do acesso à aplicação quanto no registro da conexão, tem sido considerada adequada assim como o processamento de reiterados registros sem a informação da porta.

Havendo o compartilhamento dos endereços IPv4 entre vários usuários e na ausência da informação da *porta*, não será possível identificar univocamente uma pessoa associada a uma conexão, deixando esse registro, ao menos formalmente, de ser uma informação pessoal[19], perdendo sua utilidade prática se individualmente considerado.

Questões a ser consideradas: capacidade de implementação do IPV6 (o que sem dúvida facilitaria as investigações) e capacidade técnica de os administradores de serviços autônomos de conexão à internet de manter os registros de conexão, bem como identificar as portas.

2.3.4. – INDICAÇÃO AO BANCO CENTRAL, POR INTERMÉDIO DO MINISTÉRIO DA FAZENDA, SUGERINDO A ADOÇÃO DE MEDIDAS DE COMBATE AOS CRIMES CIBERNÉTICOS – pág. 231 do Relatório e seguintes

Do relatório, destaco:

> Os trabalhos da CPI foram divididos em quatro Sub-Relatorias, uma delas a de Instituições Financeiras e Comércio Virtual, a cargo do Sub-Relator Deputado Sandro Alex. Em sua análise, essa Sub-Relatoria considerou que o combate aos crimes cibernéticos praticados contra a ordem financeira e, em especial, contra as instituições bancárias deve ser realizado com melhor atenção às informações prestadas pelas instituições reguladas e com maior integração entre as partes envolvidas como a temática.

Por esses motivos, a CPI vem oferecer esta Indicação para a instituição das seguintes medidas:

i) **Promover as medidas necessárias para a promoção de maior integração da instituição com a Polícia Federal e a Febraban para a comunicação de incidentes e o compartilhamento das informações com o objetivo de mitigar os crimes digitais;**

ii) **Propor instrumento regulatório que permita a correta aferição dos crimes cibernéticos no sistema financeiro, em separado, sem desconsiderar o caráter sensível das informações;**

iii) **Elaboração de um sistema de classificação de risco das instituições financeiras que permita aos cidadãos escolher seus prestadores de serviços financeiros e bancários com base em informações que avaliem a incidência de crimes cibernéticos nas instituições, sem desconsiderar o caráter sensível das informações.**

Acho bastante improvável que as instituições financeiras concordem com a criação de um sistema de classificação de riscos baseada na ocorrência de crimes cibernéticos; de outro lado, há que se definir o que seria uma "maior integração da instituição com a Polícia Federal e Febraban para a comunicação de incidentes", e se isto afetaria a intimidade dos correntistas.

Esta é uma proposta sobre a qual não é possível fazer maiores observações, a não ser que devemos acompanhar o seu desdobramento.

2.3.5. – INDICAÇÃO AO MINISTRO DA JUSTIÇA SUGERINDO A ADOÇÃO DE MEDIDAS DE COMBATE AOS CRIMES CIBERNÉTICOS. – pág. 232 do Relatório e seguintes

Destaco do Relatório:

Por esses motivos, a CPI vem oferecer esta Indicação para a criação de Grupo de Trabalho no âmbito dessa instituição com o seguinte escopo:

i) **Promover as medidas necessárias para a promoção de maior integração da Polícia Federal com o Banco Central para a comunicação de incidentes e o compartilhamento das informações com o objetivo de mitigar os crimes digitais e, em especial, estabelecer entendimentos para o compartilhamento das informações e a manutenção de um Banco (de Dados) Nacional de Fraudes Bancárias;**

ii) **Regulamentar o inciso VI, do art. 1º da Lei no 10.446/02, Lei das Infrações Federais, obrigando a entrega pelos bancos de notícia crime em casos de crimes cibernéticos.**

iii) **Sugere-se o estabelecimento de convênios entre as polícias federal e civis dos Estados para eventual aplicação de receitas do Fistel, transferidas para o Tesouro Nacional, no financiamento das estruturas de combate a crimes cibernéticos**

A lei mencionada acima dispõe:

Art. 1º Na forma do inciso I do § 1º do art. 144 da Constituição, quando houver repercussão interestadual ou internacional que exija repressão uniforme, poderá o Departamento de Polícia Federal do Ministério da Justiça, sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no art. 144 da Constituição Federal, em especial das Polícias Militares e Civis dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais:

I – [...]

II – [...]

III – [...]

IV – [...]

V - [...]

VI - furto, roubo ou dano contra instituições financeiras, incluindo agências bancárias ou caixas eletrônicos, quando houver indícios da atuação de associação criminosa em mais de um Estado da Federação.

Da mesma forma que no item acima, acho bastante improvável que as instituições financeiras não vejam problemas em prestar as informações aqui pretendidas.

Novamente, devemos acompanhar o seguimento dos trabalhos.

2.4. PROPOSTAS INÓCUAS

2.4.1 Projeto de lei que possibilita o bloqueio de aplicações de internet por ordem judicial

Certamente haverá duras críticas ao fato de este item estar inserido nas "propostas inócuas". No entanto, acredito que este é um projeto de lei em que há um grande equívoco: a CPI que o propôs e os seus críticos, alguns dos quais alegam que tal inserção no Marco Civil feriria a neutralidade da rede.

O que é neutralidade da rede? Grosso modo, é a obrigação de as empresas que ofertam serviços de conexão à internet tratarem de modo isonômico os pacotes de dados que trafegam na rede. Colocando em termos mais simples, as empresas não podem decidir que o envio de email deve ter tratamento de tráfego diferente da Netflix, nem podem decidir que determinado site não deve ser acessado. Está certo.

As empresas não podem mesmo filtrar pacotes de dados com base no seu conteúdo, origem e destino. AS EMPRESAS. O juiz? Ah, este pode sim, e não precisa deste projeto de lei proposto. O juiz JÁ PODE determinar esta filtragem, e isto não tem qualquer relação com neutralidade da rede, e sim **com sanção a ato ilícito**.

É um princípio basilar do Direito: ao juiz, quando provocado, cumpre decidir a forma correta de aplicar a lei. Nos casos em que o juiz entende que determinada lei não está sendo cumprida de forma adequada, ou ainda, que alguém está violando a lei, ou desrespeitando ordem proferida pelo Judiciário, ele não só pode como DEVE impor uma sanção àquele que descumpre a lei.

Não estamos falando aqui de neutralidade de rede; não se trata de empresas privilegiando tráfego: estamos falando de ILÍCITOS que devem ser punidos.

O Marco Civil não alterou o alcance do poder dos juízes, tampouco alterou a Constituição (nem poderia); desta forma, ainda que este projeto de lei seja vetado, o Poder Judiciário tem sim o condão de determinar o bloqueio de determinado site.

E antes que mencionem o caso do Whatsapp, adianto: a reversão da ordem de suspensão não se deu porque o juiz não teria poderes para determinar o bloqueio, mas sim porque o desembargador entendeu que a medida era excessiva. É importante que se faça tal distinção.

Ressalte-se também, por amor à argumentação, que o próprio Marco Civil já dispõe de artigo determinando bloqueio de acesso em alguns casos, deixando claro que a relação não é estanque, podendo ser aplicadas outras sanções cabíveis:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> **III - suspensão temporária das atividades que envolvam os atos previstos no art. 11**; ou
>
> **IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11**.
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

REDAÇÃO ATUAL DO MARCO CIVIL	SUGESTÃO DE REDAÇÃO PELA CPI
Art. 9o O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. § 1o A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de: I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e II - priorização de serviços de emergência. § 2o Na hipótese de discriminação ou degradação do tráfego prevista no § 1o, o responsável mencionado no caput deve: I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil; II - agir com proporcionalidade, transparência e isonomia; III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais. **§ 3o Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.**	"Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. **§ 4º Ordem judicial poderá determinar aos provedores de conexão bloqueio ao acesso a aplicações de internet por parte dos usuários, sempre que referida medida for implementada com a finalidade de coibir o acesso a serviços que, no curso do processo judicial, forem considerados ilegais." (NR)**

À página 137, a CPI incorre na mesma incorreção quando menciona que é necessário que a nova Lei de Direitos Autorais preveja a possibilidade de o juiz determinar bloqueio ao acesso a aplicações de internet que infrinjam direitos autorais de forma contumaz. Gostaria novamente de lembrar que ao juiz de Direito já é dado este poder, dentro de determinados limites e condições. Basicamente, este projeto pretende inserir no Marco Civil que o juiz pode sim determinar uma ordem judicial, o que me parece um projeto de lavra do Conselheiro Acácio.

3. CONCLUSÃO:

Como pode-se verificar pela análise acima, apesar de haver vários pontos críticos que merecem vigilância estreita da sociedade, a CPI dos Crimes Cibernéticos fez um bom trabalho e não deve ser de todo rejeitada.

Estamos vivendo um período político e social no qual a polarização é rainha, onde só há preto e branco, onde não há matizes de cinza, onde pontes são destruídas ao invés de construídas.

Acredito que com uma discussão madura dos temas propostos durante o processo legislativo possamos colher bons frutos desta CPI. Mas, como sempre, há que se ter boa vontade.